

THÈSE

présentée

A LA FACULTÉ DES SCIENCES ET DES TECHNIQUES DE
L'UNIVERSITÉ DE FRANCHE-COMTÉ

pour obtenir le

GRADE de DOCTEUR ES SCIENCES MATHÉMATIQUES

par

Bernard ORIAT

ESSAI

DE GÉNÉRALISATION DU "SPIEGELUNGSSATZ"



Soutenue le 29 septembre 1980, devant la Commission d'Examen :

MM.	J.J. PAYAN , Professeur à l'Université de Grenoble I	Président
	G. GRAS , Professeur à l'Université de Franche-Comté	Directeur de Recherche
	J.P. BERTRANDIAS , Professeur à l'Université de Grenoble I	} Examineurs
	J. COUGNARD , Professeur à l'Université de Franche-Comté	
	P. KAPLAN , Professeur à l'Université de Nancy I	

THÈSE

présentée

A LA FACULTE DES SCIENCES ET DES TECHNOLOGIES DE
L'UNIVERSITÉ DE FRANCHE-COMTE

pour obtenir le

GRADE de DOCTEUR ES SCIENCES MATHÉMATIQUES

Digitized by the Internet Archive
in 2026

Bernard ORLAT

ESSAI

DE GÉNÉRALISATION DU "SPIEGELUNGSSATZ"



Soutenue le 29 septembre 1990, devant la Commission d'Examen :

M. J. J. PAVAN, Professeur à l'Université de Franche-Comté

Président

M. BRAS, Professeur à l'Université de Franche-Comté

Directeur de Recherche

THÈSE

présentée

A LA FACULTÉ DES SCIENCES ET DES TECHNIQUES DE
L'UNIVERSITÉ DE FRANCHE-COMTÉ

pour obtenir le

GRADE de DOCTEUR ES SCIENCES MATHÉMATIQUES

par

Bernard ORIAT

ESSAI

DE GÉNÉRALISATION DU "SPIEGELUNGSSATZ"



Soutenue le 29 septembre 1980, devant la Commission d'Examen :

MM.

J.J. PAYAN, Professeur à l'Université de Grenoble I

G. GRAS, Professeur à l'Université de Franche-Comté

J.P. BERTRANDIAS, Professeur à l'Université de Grenoble I

J. COUGNARD, Professeur à l'Université de Franche-Comté

P. KAPLAN, Professeur à l'Université de Nancy I

Président

Directeur de Recherche

Examineurs

THÈSE

A LA FACULTÉ DES SCIENCES ET DES TECHNIQUES DE
L'UNIVERSITÉ DE BRUXELLES

PAR

GRACE DE DOCTEUR EN SCIENCES MATHÉMATIQUES

GRACE DE DOCTEUR



DE GÉNÉRALISATION DU "SPIEGELUNGSSATZ"

UNIVERSITÉ DE FRANCHE-COMTÉ BESANÇON

Président : Monsieur le Professeur Pierre LÉVÊQUE

Président honoraire : Monsieur le Professeur Jean THIÉBAUT

FACULTÉ DES SCIENCES ET DES TECHNIQUES

DOYEN

M. le Professeur Jean BULABOIS
Physique Générale-optique

ASSESEURS

M. le Professeur Bernard MILLET
Botanique
M. Robert GUYETANT, Maître-Assistant
Biol. animale Ecologie

DOYENS HONORAIRES

MM. GLANGEAUD, JACQUEMAIN, CHATELET,
THIEBAUT, BERNARD

PROFESSEURS HONORAIRES

MM. BENNETON, CHATELET, MESNAGE, QUANTIN
THEOBALD N., THIRY, TRILLAT, TRONCHET,
UEBERSFELD

MM. BANTEGNIE Robert	: Mathématiques	MIELLOU J. Claude	: Analyse numérique
BENILAN Philippe	: Mathématiques	MILLET Bernard	: Botanique
BERNARD Jean	: Chimie Physique	MONTAGNER Hubert	: Psychophysiologie
BIDAULT Michel	: Taxonomie expérimentale	MOREELS Guy	: Astronomie
BROQUET Paul	: Géologie	OLIVIER Marcel	: Electroniq. quantique
BRUCKERT Sylvain	: Ecologie végétale	PARIZET Jean	: Mathématiques
BULABOIS Jean	: Physique Gle optique	PERROT Roger	: Chimie générale
CAPODANNO Pierre	: Mécanique théorique	PLUVINAGE Philippe	: Physique théorique
CERUTTI Ernest	: Chimie appliquée	POTIER Robert	: Physique des sols
CHALEAT Raymond	: Mécanique appliquée	RANGHEARD Yves	: Géologie
CHARDON J. Claude	: Spectroscopie	REAL Pierre	: Ecologie animale
CHAUVE Pierre	: Géologie minéralogie	RIPPLINGER Jean	: Physiologie animale
COUGNARD Jean	: Mathématiques	ROBERT Daniel	: Physique
DEVIN Claude	: Chimie 1er cycle	ROBERT Guy	: Electrochimie
DUBOUCHET Jacques	: Physiologie végétale	ROBERT Jacques	: Mathématiques I
GALATRY Louis	: Physique moléculaire	THEOBALD J. Gérard	: Spectroscopie hertzienne
GAUDEMER Yves	: Biochimie	THIEBAUT Jean	: Pétrogr.minéralogie
GOMOT Lucien	: Zoologie-Embryologie	TREHEL Michel	: Informatique
GOUARNE René	: Mathématiques	VERNEAUX Jean	: Zoologie-Embryologie
GRAS Georges	: Mathématiques	VIENTOT J.Charles	: Physique Gle optique
GREMILLARD Jean	: Mathématiques	WEIL Michel	: Mathématiques
KARCHE J.Paul	: Pétrographie Minéralogie		
LALLEMENT Gérard	: Mécanique appliquée		
LAUDE Bernard	: Chimie organique		
LESANT Pierre	: Mathématiques I		
LHOTE François	: Automatique		
MERIGOUX Henri	: Cristallographie et Synthèses minérales		

Responsable des services administratifs :
M. Jean-Marie RUNGE

J'exprime ici ma profonde reconnaissance à Georges Gras. Sans la constante disponibilité dont il a fait preuve à mon égard et les conseils qu'il m'a prodigués, jamais ce travail n'aurait vu le jour.

Monsieur le Professeur Jean-Jacques Payan m'a fait l'honneur de présider le jury. Je l'en remercie sincèrement.

Jean Cougnard et Pierre Kaplan ont répondu avec bienveillance à mes questions et m'ont encouragé par leurs suggestions. Je leur adresse mes plus vifs remerciements.

Je remercie également Monsieur le Professeur Jean-Paul Bertrandias qui m'a proposé un second sujet.

Je n'aurai garde d'oublier les membres du Laboratoire qui, par leur attitude amicale, ont su créer une atmosphère chaleureuse, favorable à ma recherche.

Je veux enfin remercier toutes les personnes qui, au secrétariat de Mathématiques ou à l'imprimerie de la Faculté ont contribué à la réalisation matérielle de ce travail.

LISTE DES PUBLICATIONS COMPOSANT LA THESE
=====

- (I) Spiegelungssatz, Publications Mathématiques de la Faculté des Sciences de Besançon (1975-1976).
- (II) Relation entre les 2-groupes des classes d'idéaux au sens ordinaire et restreint de certains corps de nombres, Bull. Soc. Math. France, 104 (1976).
- (III) Relations entre les 2-groupes des classes d'idéaux des extensions quadratiques $k(\sqrt{d})$ et $k(\sqrt{-d})$, Ann. Inst. Fourier, Grenoble, 27, 2 (1977).
- (IV) 2, 4 et 8-rang du groupe des classes d'idéaux de $\mathbb{Q}(\sqrt{2}, \sqrt{d})$, $|d| \leq 1000$, Publications Mathématiques de la Faculté des Sciences de Besançon (1975-1976).
- (V) Sur la divisibilité par 8 et 16 des nombres de classes d'idéaux des corps quadratiques $\mathbb{Q}(\sqrt{2p})$ et $\mathbb{Q}(\sqrt{-2p})$, J. Math. Soc. Japan, vol. 30, 2 (1978).
- (VI) Un essai de généralisation du "Spiegelungssatz" (en collaboration avec Ph. Satgé), J. für die reine und ang. Math. 307/308 (1979).
- (VII) Généralisation du "Spiegelungssatz", Astérisque, 61 (1979).
- (VIII) "Spiegelungssatz" et $\mathbb{Z}_\ell$ -extensions, non publié.
- (IX) Annulation de groupes de classes réelles, Nagoya Math. J. 81 (1981).

ESSAI DE GENERALISATION DU "SPIEGELUNGSSATZ"

Les travaux qui composent cette thèse portent tous sur le même thème : généraliser le "Spiegelungssatz" de H. W. Leopoldt [13]. Ils reposent tous sur l'utilisation de la "Spiegelungsrelation". Afin de dégager l'unité de ce travail, nous présentons d'abord cette propriété.

1 SPIEGELUNGSRELATION

Nous désignons par ℓ un nombre premier, par n une puissance de ℓ , par A_n l'anneau $\mathbb{Z}/n\mathbb{Z}$ des classes résiduelles d'entiers modulo n . Soit L/k une extension galoisienne finie de corps de nombres et soit G son groupe de Galois. On suppose que L contient une racine primitive $n^{\text{ème}}$ de l'unité. Soit M/L une extension abélienne finie, d'exposant divisant n , telle que M/k soit galoisienne. Il s'agit d'une extension de Kummer, dont le radical (c'est-à-dire l'ensemble des éléments de L tels que leurs racines $n^{\text{ème}}$ appartiennent à M) est désigné par W . Soit L^* le groupe multiplicatif du corps L et soit $\langle \zeta_n \rangle$ le groupe engendré par ζ_n , racine primitive $n^{\text{ème}}$ de 1. En vertu de la théorie classique de Kummer, le groupe W/L^{*n} est canoniquement isomorphe à $\text{Hom}(\text{Gal}(M/L), \langle \zeta_n \rangle)$. Nous désignons par α cet isomorphisme et nous rappelons sa définition : si u appartient à $\text{Gal}(M/L)$ et w à W , alors $\alpha(wL^{*n})(u) = \left(\sqrt[n]{w}\right)^{u-1}$ (nous notons exponentiellement l'action des groupes de Galois. En conséquence, la composition des automorphismes u et v est notée suivant la règle $x^{uv} = (x^u)^v$).

Le groupe W/L^{*n} est un G -module, l'action de G étant définie par $(wL^{*n})^\tau = w^\tau L^{*n}$ pour tout τ de G . Le groupe G opère également sur $\text{Gal}(M/L)$ par conjugaison : si t est un prolongement à M de l'élément τ de G et si u appartient à $\text{Gal}(M/L)$, on pose $u^\tau = t^{-1} u t$.

Nous notons A_n^* l'ensemble des classes résiduelles d'entiers modulo n , premières à ℓ . Soit χ^* l'homomorphisme de G dans A_n^* , tel que $\zeta_n^{\chi^*(\tau)} = \zeta_n^\tau$ pour tout τ de G . Si x est un élément de $A_n[G]$ de la forme $x = \sum_{\tau \in G} a_\tau \tau$, on note

$\bar{x} = \sum_{\tau \in G} a_{\tau} \chi^*(\tau) \tau^{-1}$. L'application qui à x fait correspondre $\bar{x}$ est un anti-isomorphisme involutif de $A_n[G]$. On l'appelle "involution du miroir". Les structures de $A_n[G]$ -module de W/L^{*n} et $\text{Gal}(M/L)$ sont liées par la "Spiegelungsrelation" qui s'énonce ainsi :

Théorème : Pour tout w de W , tout x de $A_n[G]$ et tout u de $\text{Gal}(M/L)$ on a l'égalité :

$$\alpha((wL^{*n})^x)(u) = \alpha(wL^{*n})(u\bar{x}).$$

La démonstration de cette propriété est élémentaire et est écrite dans [13]. On la trouve aussi dans [7].

On peut être tenté d'utiliser des $\mathbb{Z}_{\ell}[G]$ -modules au lieu de $A_n[G]$ -modules. Enonçons la "Spiegelungsrelation" dans ce cadre : soit, si ℓ est impair, ζ_{ℓ} une racine primitive $\ell^{\text{ème}}$ de 1. On note χ^{**} l'homomorphisme de G dans $\mathbb{Z}_{\ell}^*$, groupe des unités de $\mathbb{Z}_{\ell}$, tel que $\zeta_{\ell}^{\chi^{**}(\tau)} = \zeta_{\ell}^{\tau}$ pour tout τ de G . Lorsque $\ell = 2$ et $n \geq 4$, on désigne par ζ_4 une racine primitive $4^{\text{ème}}$ de 1 et par χ^{**} l'homomorphisme de G dans $\mathbb{Z}_2^*$ tel que $\zeta_4^{\chi^{**}(\tau)} = \zeta_4^{\tau}$. Si $n = 2$, on peut convenir de choisir χ^{**} trivial. A partir de χ^{**} , on peut définir une involution de $\mathbb{Z}_{\ell}[G]$ de la même façon : si $x = \sum_{\tau \in G} a_{\tau} \tau$ est un élément de $\mathbb{Z}_{\ell}[G]$, on pose $\bar{x} = \sum_{\tau \in G} a_{\tau} \chi^{**}(\tau) \tau^{-1}$. Les structures de $\mathbb{Z}_{\ell}[G]$ -modules de W/L^{*n} et $\text{Gal}(M/L)$ ne seront liées par la relation : $\alpha((wL^{*n})^x)(u) = \alpha(wL^{*n})(u\bar{x})$, pour tout x appartenant à $\mathbb{Z}_{\ell}[G]$, que si $\chi^*(\tau)$ est le résidu de $\chi^{**}(\tau)$ modulo n , pour tout τ de G . Introduisons, pour examiner cette condition, la $\mathbb{Z}_{\ell}$ -extension $\mathbb{Q}_{\infty}$ de $\mathbb{Q}$ et l'intersection $\mathbb{Q}_{(n)} = \mathbb{Q}_{\infty} \cap \mathbb{Q}^{(n)}$; où $\mathbb{Q}^{(n)}$ désigne, comme d'habitude, le corps cyclotomique $\mathbb{Q}(\zeta_n)$. On vérifie alors :

Proposition : La condition : $\chi^*(\tau)$ est le résidu modulo n de $\chi^{**}(\tau)$ pour tout τ de G , est équivalente à la condition : $\mathbb{Q}_{(n)} \subset k$. Si cette condition est vérifiée, alors la Spiegelungsrelation peut s'écrire en termes de $\mathbb{Z}_{\ell}[G]$ -modules :

$\alpha((wL^{*n})^x)(u) = \alpha(wL^{*n})(u\bar{x})$, pour tout w de W , tout u de $\text{Gal}(M/L)$, tout x de $\mathbb{Z}_{\ell}[G]$.

2 PRINCIPE D'UTILISATION DE LA SPIEGELUNGSRELATION

La propriété énoncée plus haut est utilisée dans tout ce qui suit ainsi : l'extension M/L est non ramifiée ; son groupe de Galois est donc par la théorie du corps de classe, isomorphe en tant que G -module à un groupe quotient du groupe des classes d'idéaux de L . Plus souvent, M est obtenue par composition avec L d'une extension N/K abélienne non ramifiée d'un corps K situé entre L et k . Ainsi c'est un quotient d'un groupe de classes d'idéaux d'un corps intermédiaire K qui intervient.

Si w appartient à W , alors l'idéal qu'il engendre est une puissance $n^{\text{ème}}$ d'un idéal $\mathfrak{a}$ de L . En associant à w la classe de $\mathfrak{a}$, on définit une application de W/L^{*n} dans le groupe des classes de L . Si wL^{*n} est invariant par l'action d'un sous-groupe : $\text{Gal}(L/\bar{K})$ de G , $\bar{K}$ étant un corps situé entre L et k , il en est de même de la classe de $\mathfrak{a}$. Dans ce cas, on cherche à faire intervenir, non plus le groupe des classes d'idéaux de L , mais le groupe des classes d'idéaux de $\bar{K}$. Les applications qui relient le radical W et le groupe des classes de L (ou de $\bar{K}$) sont notées θ . Les noyaux de ces applications θ s'expriment le plus souvent à l'aide d'unités du corps L (ou du corps $\bar{K}$). On dispose ainsi d'un moyen de relier un quotient du groupe des classes d'idéaux de L (ou de K), un sous-groupe du groupe des classes d'idéaux de L (ou de $\bar{K}$) et un groupe d'unités de L (ou de $\bar{K}$). La Spiegelungsrelation intervient dans les définitions de ces trois groupes : en effet, si un élément x de $A_n[G]$ annule le groupe quotient considéré, alors $\bar{x}$ annule les deux autres groupes : groupe des classes d'idéaux de $\bar{K}$ et groupe d'unités de $\bar{K}$.

3 TRAVAUX ANTERIEURS

La Spiegelungsrelation fut d'abord utilisée ainsi par H. W. Leopoldt dans [13]. Ce dernier a choisi $n=\ell$, $k=\mathbb{Q}$, et a posé l'hypothèse suivante : " ℓ ne divise pas le degré $[L:\mathbb{Q}]$ ". Cette hypothèse permet de définir les groupes de classes et d'unités utilisés à l'aide d'idempotents. Soit ϕ un caractère ℓ -adique de G et $1_\phi = (1/[L:\mathbb{Q}]) \sum_{\tau \in G} \phi(\tau) \tau^{-1}$ l'idempotent de $\mathbb{Q}_\ell[G]$ associé à ϕ . Il appartient en fait à $\mathbb{Z}_\ell[G]$ et il y a une correspondance biunivoque entre les idempotents de $\mathbb{Q}_\ell[G]$ et les idempotents de $\mathbb{F}_\ell[G]$ déduite de l'application canonique

de $\mathbb{Z}_\ell[G]$ sur $\mathbb{F}_\ell[G]$. L'application χ^* est le résidu modulo ℓ de χ^{**} et la Spiegelungsrelation peut s'écrire en termes de $\mathbb{Z}_\ell[G]$ -module ou en termes de $\mathbb{F}_\ell[G]$ -modules. Posons $\bar{\phi} = \chi^{**} \phi^-$, ϕ^- étant défini par : $\phi^-(\tau) = \phi(\tau^{-1})$ pour tout τ de G . C'est un caractère ℓ -adique de G . L'application $\phi \rightarrow \bar{\phi}$ est une involution de l'ensemble des caractères ℓ -adiques de G . Les idempotents associés à ϕ et $\bar{\phi}$, notés 1_ϕ et $1_{\bar{\phi}}$, se correspondent par l'involution du miroir.

Soit $\mathcal{K}(L)$ le groupe des ℓ -classes d'idéaux de L et, si $E(L)$ est le groupe des unités de L , soit $\mathcal{E}(L) = E(L)/E(L)^\ell$. Les groupes de classes d'idéaux et d'unités considérés ici sont $\mathcal{K}(L)^{1_\phi}$, $\mathcal{K}(L)^{1_{\bar{\phi}}}$ et $\mathcal{E}(L)^{1_{\bar{\phi}}}$. Désignons par $\dim_\ell$ le ℓ -rang. Le théorème suivant est énoncé dans [13] et porte le nom de "Spiegelungssatz" :

Théorème : Si ℓ ne divise pas le degré $[L : \mathbb{Q}]$ et si ϕ est un caractère ℓ -adique de G , alors on a l'inégalité :

$$\dim_\ell \mathcal{K}(L)^{1_\phi} - \dim_\ell \mathcal{K}(L)^{1_{\bar{\phi}}} \leq \dim_\ell \mathcal{E}(L)^{1_{\bar{\phi}}}.$$

Certains cas particuliers de ce résultat avaient été l'objet d'énoncés antérieurs. Prenons par exemple : $L = \mathbb{Q}(\sqrt{d}, \sqrt{-3})$, d étant un entier sans facteur carré, positif. Si ϕ est le caractère quadratique de L , réel, il correspond au corps quadratique $\mathbb{Q}(\sqrt{d})$ et $\bar{\phi}$ est le caractère quadratique correspondant au corps $\mathbb{Q}(\sqrt{-3d})$. Le groupe des classes d'idéaux $\mathcal{K}(L)^{1_\phi}$ est le 3-groupe des classes d'idéaux de $\mathbb{Q}(\sqrt{d})$. Notons le $\mathcal{K}(\mathbb{Q}(\sqrt{d}))$. De même, $\mathcal{K}(L)^{1_{\bar{\phi}}}$ est le groupe $\mathcal{K}(\mathbb{Q}(\sqrt{-3d}))$ des 3-classes d'idéaux de $\mathbb{Q}(\sqrt{-3d})$. En appliquant deux fois le théorème précédent, nous obtenons les inégalités :

$$0 \leq \dim_3 \mathcal{K}(\mathbb{Q}(\sqrt{-3d})) - \dim_3 \mathcal{K}(\mathbb{Q}(\sqrt{d})) \leq 1.$$

Ce résultat est du à Scholz [14].

L'hypothèse " ℓ ne divise pas $[L : k]$ " faite en [13] permet de définir les groupes de classes d'idéaux et d'unités considérés : $\mathcal{K}(L)^{1_\phi}$ et $\mathcal{E}(L)^{1_\phi}$. Si cette hypothèse n'est plus faite, l'idempotent 1_ϕ n'est plus dans $\mathbb{Z}_\ell[G]$ et les notations $\mathcal{K}(L)^{1_\phi}$ et $\mathcal{E}(L)^{1_\phi}$ n'ont plus de sens. Nous avons essayé de ne plus utiliser cette hypothèse. Nous y avons été incité par le travail de Damey et Payan [3]. Il y est démontré que si d est un entier sans facteur carré positif et si $\mathcal{K}(\mathbb{Q}(\sqrt{d}))$ et $\mathcal{K}(\mathbb{Q}(\sqrt{-d}))$ sont les 2-groupes de classes d'idéaux de $\mathbb{Q}(\sqrt{d})$ et $\mathbb{Q}(\sqrt{-d})$, alors les

4-rangs de ces groupes sont liés par la relation :

$$0 \leq \dim_4 \mathcal{H}(\mathbb{Q}(\sqrt{-d})) - \dim_4 \mathcal{H}(\mathbb{Q}(\sqrt{d})) \leq 1.$$

La ressemblance avec la propriété de Scholz est flagrante. Mais il est sûr qu'il ne s'agit pas d'un cas particulier du théorème énoncé ci-dessus, car les groupes des classes d'idéaux des corps quadratiques considérés ne peuvent être définis à l'aide d'idempotents.

4 RESUME DES TRAVAUX CONSTITUANT LA THESE

Dans (I) nous avons présenté le "Spiegelungssatz" de H. W. Leopoldt [13]. La seule différence consiste à prendre un corps de base k quelconque. Ceci permet de considérer non seulement le ℓ -rang des groupes de classes d'idéaux, mais aussi les m -rangs de ces groupes ; m désignant une puissance de ℓ telle que L contienne une racine primitive $m^{\text{ème}}$ de 1. Nous supposons toujours que ℓ ne divise pas le degré de l'extension L/k . Dans ces conditions $\chi^*(\tau)$ est, pour tout τ de G , le résidu modulo n de $\chi^{**}(\tau)$. Les groupes de classes d'idéaux et d'unités sont définis de la même façon, à l'aide d'idempotents. Le résultat obtenu a la même forme qu'en [13].

Dans (II), nous nous sommes intéressés au cas très particulier où $n = \ell = 2$. Dans ce cas les applications χ^* et χ^{**} sont triviales et l'involution du miroir de $\mathbb{Z}_2[G]$ est le prolongement de l'involution de G définie par $\tau \rightarrow \tau^{-1}$. Nous prenons $k = \mathbb{Q}$ et supposons vérifiée l'hypothèse : "2 ne divise pas le degré $[L : \mathbb{Q}]$ ". Soit ϕ un caractère 2-adique irréductible de G . Dans ce cadre le caractère $\bar{\phi}$ coïncide avec ϕ^- . Nous considérons non seulement le 2-groupe des classes au sens ordinaire de L , noté $\mathcal{H}'(L)$ mais aussi le 2-groupe des classes au sens restreint de L , noté $\mathcal{H}(L)$. Les groupes de classes d'idéaux étudiés sont définis comme précédemment à l'aide des idempotents 1_ϕ et $1_{\bar{\phi}}$ associés à ϕ et $\bar{\phi}$. Nous obtenons ainsi, en utilisant le même principe, une relation entre ces groupes de classes. Si l'on désigne par χ le caractère absolument irréductible de G au-dessus de ϕ et par $\dim_2$ le 2-rang, cette relation s'énonce :

Théorème : Si ϕ est un caractère irréductible de G sur $\mathbb{Q}_2$, on a :

$$\dim_2 \mathcal{H}(L)^{1_\phi} - \dim_2 \mathcal{H}'(L)^{1_\phi} + \dim_2 \mathcal{H}(L)^{1_{\bar{\phi}}} - \dim_2 \mathcal{H}'(L)^{1_{\bar{\phi}}} \leq \phi(1)\chi(1).$$

Remarquons que le 2-rang d'un $\mathbb{Z}_2[G]$ -module de la forme $\mathcal{H}(L)^{1_\phi}$ est un

multiple de $\phi(1)$. Dans le cas particulier où G est abélien, $\chi(1)$ vaut 1 et cette propriété peut s'écrire plus simplement sous la forme : l'une ou l'autre des égalités suivantes est vraie :

$$\dim_2 \mathcal{X}(L)^{1_\phi} = \dim_2 \mathcal{X}'(L)^{1_\phi}, \quad \dim_2 \mathcal{X}(L)^{1_{\bar{\phi}}} = \dim_2 \mathcal{X}'(L)^{1_{\bar{\phi}}}.$$

Nous retrouvons ainsi les résultats obtenus par Armitage et Fröhlich dans [1].

Dans (III), nous nous sommes intéressés à la propriété [3] de Damey et Payan. Nous en avons donné une démonstration qui utilise le principe décrit ci-dessus au § 2. Nous avons pu obtenir ainsi un énoncé un peu plus général. Soient n une puissance de 2 supérieure à 4, k un corps de base, d un élément de k non carré dans k . Nous considérons les corps $K = k(\sqrt{d})$, $\bar{K} = k(\sqrt{-d})$ et $L = K(\sqrt{d}, \sqrt{-d})$. Nous supposons que k contient $\mathbb{Q}_o^{(n)}$ sous-corps réel maximal du $n^{\text{ème}}$ corps cyclotomique. Soient $\mathcal{X}(K)$, $\mathcal{X}(\bar{K})$ et $\mathcal{X}(k)$ les 2-groupes de classes d'idéaux au sens restreint de K , $\bar{K}$ et k . Soient j et $\bar{j}$ les applications de $\mathcal{X}(k)$ dans $\mathcal{X}(K)$ et $\mathcal{X}(\bar{K})$ déduites des injections canoniques du groupe des idéaux de k dans les groupes d'idéaux de K et $\bar{K}$. Ici nous ne pouvons plus employer d'idempotents et les groupes des classes d'idéaux considérés sont $\mathcal{J}$ et $\bar{\mathcal{J}}$ définis par $\mathcal{J} = \mathcal{X}(K)/j(\mathcal{X}(k))$ et $\bar{\mathcal{J}} = \mathcal{X}(\bar{K})/\bar{j}(\mathcal{X}(k))$.

Remarquons que ce type de définition faisant intervenir des applications "j" n'est utilisé qu'avec $\ell = 2$. Plus loin, dans le cas ℓ impair, nous poserons d'autres définitions.

Pour énoncer le résultat il est nécessaire d'introduire les notations suivantes : soient $E_{\bar{K}}$ et E_k les groupes d'unités de $\bar{K}$ et k . Soient $\dim_{\mathbb{Z}} E_{\bar{K}}$ et $\dim_{\mathbb{Z}} E_k$ les dimensions des $\mathbb{Z}$ -modules quotients de $E_{\bar{K}}$ et E_k par leurs sous-groupes de torsion. On pose $n_1 = \dim_{\mathbb{Z}} E_{\bar{K}} - \dim_{\mathbb{Z}} E_k$. Soient E_k^+ et $E_{\bar{K}}^+$ l'ensemble des éléments totalement positifs de E_k et $E_{\bar{K}}$. Nous désignons par n_2 le 2-rang du groupe $(E_k^+ \cap N_{\bar{K}/k}(\bar{K}))/E_k^2 N_{\bar{K}/k}(E_{\bar{K}}^+)$. Soit $\mathcal{X}(k)^{(2)}$ l'ensemble des éléments h de $\mathcal{X}(k)$ tels que $h^2 = 1$ et soit P_k le sous-groupe de $\mathcal{X}(k)$ engendré par les idéaux principaux au sens ordinaire. On désigne par n_3 le 2-rang du groupe $\mathcal{X}_k^{(2)}/(\text{Ker } \bar{j} \cdot P_k)$.

Nous avons démontré dans (III) le résultat suivant :

Théorème : Soit m une puissance de 2 comprise entre 4 et n . La différence des m -rangs de $\mathcal{J}$ et $\bar{\mathcal{J}}$ est majorée de la façon suivante :

$$\dim_m \mathcal{J} - \dim_m \bar{\mathcal{J}} \leq n_1 + n_2 + n_3.$$

Dans le cas particulier où k est totalement réel et 2-principal, n_2 et n_3 sont nuls. C'est ce qui se produit avec $k = \mathbb{Q}(\sqrt{2})$. Si a est un entier sans facteur carré positif, nous avons les inégalités :

$$0 \leq \dim_4 \mathcal{H}(k(\sqrt{-a})) - \dim_4 \mathcal{H}(k(\sqrt{a})) \leq 2$$

$$0 \leq \dim_8 \mathcal{H}(k(\sqrt{-a})) - \dim_8 \mathcal{H}(k(\sqrt{a})) \leq 2.$$

Dans (IV) nous avons effectué quelques calculs numériques dans l'espoir de vérifier que les inégalités énoncées ci-dessus décrivent toutes les situations possibles. Mais nous n'avons pas trouvé de valeurs de a telles que la différence des 4-rangs soit égale à 0 et la différence des 8-rangs égale à 2. Ces calculs des 4 et 8-rangs des groupes des classes de $\mathbb{Q}(\sqrt{2}, \sqrt{\pm a})$ ont été effectués à l'aide de la méthode développée par G. Gras dans [5].

En considérant le cas particulier où a est un nombre premier p , nous avons pu dans (V) montrer un résultat concernant les corps quadratiques $\mathbb{Q}(\sqrt{2p})$ et $\mathbb{Q}(\sqrt{-2p})$ qui s'énonce ainsi :

Proposition : Si p est congru à 1 modulo 8 et si le nombre de classes d'idéaux (au sens restreint) de $\mathbb{Q}(\sqrt{2p})$ est divisible par 16, alors il en est de même du nombre de classes d'idéaux de $\mathbb{Q}(\sqrt{-2p})$.

Ce résultat précise le travail de P. Kaplan [10]. Remarquons que, par des voies analytiques, des relations plus générales ont pu être obtenues : [8] et [12].

Dans (VI) nous avons essayé de généraliser le "Spiegelungssatz" dans le cas ℓ impair. Ce travail a été réalisé en collaboration avec Ph. Satgé. L'extension L/k est supposée abélienne. On suppose toujours que L contient les racines $n^{\text{ème}}$ de l'unité, n étant une puissance de ℓ . Les groupes de classes d'idéaux et d'unités considérés sont attachés à un idéal I de l'algèbre $A_n[G]$. On définit le corps K_I comme le corps intermédiaire entre L et k tel que $\text{Gal}(L/K_I)$ soit égal à l'ensemble des σ de G tels que $\sigma-1$ appartienne à I . Si $\mathcal{H}(K_I)$ est le ℓ -groupe des classes d'idéaux de K_I , le groupe $\mathcal{H}^I$ est le plus grand quotient de $\mathcal{H}(K_I)/\mathcal{H}(K_I)^n$

annulé par I . De même, si $\mathcal{H}(K_I)^{(n)}$ est le sous-groupe de $\mathcal{H}(K_I)$ formé des éléments h de $\mathcal{H}(K_I)$ tels que $h^n = 1$, $\mathcal{H}_I$ est défini comme le plus grand sous-groupe de $\mathcal{H}(K_I)^{(n)}$ annulé par I .

Remarque : Ces définitions généralisent les définitions qui utilisaient des idempotents : en effet si ℓ ne divise pas $[L : k]$, si ϕ est un caractère ℓ -adique de G et si 1_ϕ est l'idempotent correspondant, soit I l'idéal de $A_n[G]$ engendré par le résidu modulo n de $1 - 1_\phi$. On vérifie immédiatement que $\mathcal{H}^I$ et $\mathcal{H}_I$ sont isomorphes à $\mathcal{H}(L)^{1_\phi} / (\mathcal{H}(L)^{1_\phi})^n$. Ainsi pour toute puissance de ℓ , notée m et comprise entre ℓ et n , $\mathcal{H}^I$, $\mathcal{H}_I$ et $\mathcal{H}(L)^{1_\phi}$ ont même m -rang.

De la même façon, on désigne par $E(K_I)$ le groupe des unités de K_I , $\mathcal{E}(K_I)$ le quotient $E(K_I)/E(K_I)^n$ et $\mathcal{E}_I$ le plus grand sous-groupe de $\mathcal{E}(K_I)$ annulé par I . Précisons enfin que $\bar{I}$ est l'image de I par l'involution du miroir de $A_n[G]$ et que le m -rang est noté $\dim_m$. Nous avons démontré dans (VI) le résultat suivant :

Théorème : Pour toute puissance de ℓ notée m et comprise entre ℓ et n , on a l'inégalité :

$$\dim_m \mathcal{H}^I - \dim_m \mathcal{H}_{\bar{I}} \leq \dim_\ell \mathcal{E}_{\bar{I}} + 1.$$

De plus si l'une ou l'autre des hypothèses suivantes est vérifiée :

- Le degré $[L : K_I]$ est premier à ℓ ,
- Le corps $K_{\bar{I}}$ ne contient pas de racine primitive $\ell^{\text{ème}}$ de 1,
- Il existe un idéal premier de K_I totalement ramifié dans L/K_I ,

alors on a plus précisément :

$$\dim_m \mathcal{H}^I - \dim_m \mathcal{H}_{\bar{I}} \leq \dim_\ell \mathcal{E}_{\bar{I}}.$$

Le changement de I en $\bar{I}$ ne permute pas $\mathcal{H}^I$ et $\mathcal{H}_{\bar{I}}$. Ainsi, obtenir une minoration de la différence $\dim_m \mathcal{H}^I - \dim_m \mathcal{H}_{\bar{I}}$ est, dans ce cadre plus général, un autre problème. Pour énoncer le résultat obtenu, introduisons un groupe d'unités locales. Soient $\ell_1, \dots, \ell_t$ les idéaux de $K_I \cap K_{\bar{I}}$ au-dessus de ℓ et D_j le groupe

de décomposition de ℓ_j dans L/k . Soit $\bar{I}(j) = A_n[D_j] \cap \bar{I}$ et soit U_j le groupe des unités principales du complété de $K_{\bar{I}}$ en un idéal au-dessus de ℓ_j . Soit $\mathcal{U}_{\bar{I}(j)}$ le plus grand sous- $A_n[D_j]$ -module de U_j/U_j^n annulé par $\bar{I}(j)$.

On mesure par s le nombre de générateurs de l'image $\bar{I}'$ de l'idéal $\bar{I}$ par l'application canonique de $A_n[G]$ sur $A_n[\text{Gal}(K_{\bar{I}}/k)]$. On désigne par $(K_I)_o$ le corps intermédiaire entre K_I et $K_I \cap K_{\bar{I}}$, maximal tel que $[(K_I)_o : K_I \cap K_{\bar{I}}]$ soit premier à ℓ . Nous avons démontré dans (VI) :

Théorème : Soit m une puissance de ℓ comprise entre ℓ et n : si le degré de l'extension $K_{\bar{I}}/k$ est premier à ℓ et si l'idéal $\bar{I}'$ est engendré par un idempotent de l'algèbre $A_n[\text{Gal}(K_{\bar{I}}/k)]$, alors on a l'inégalité :

$$\dim_m \mathcal{E}_{\bar{I}} - \sum_{j=1}^t \dim_{\ell} \mathcal{U}_{\bar{I}(j)} \leq \dim_m \mathcal{H}^I - \dim_m \mathcal{H}_{\bar{I}}.$$

Si l'une ou l'autre des hypothèses suivantes est vérifiée :

- Le corps $K_{\bar{I}}$ ne contient pas de racine de l'unité d'ordre ℓ et aucun idéal premier de $K_I \cap K_{\bar{I}}$ au-dessus de ℓ n'est totalement décomposé dans $(K_I)_o$,
- Il existe un et un seul idéal premier de K_I totalement ramifié dans L/K_I ,

alors on a l'inégalité :

$$\dim_m \mathcal{E}(K_{\bar{I}}) - s \dim_{\ell} \mathcal{E}(K_{\bar{I}}) - \sum_{j=1}^t \dim_{\ell} \mathcal{U}_{\bar{I}(j)} \leq \dim_m \mathcal{H}^I - \dim_m \mathcal{H}_{\bar{I}}.$$

On remarque que pour obtenir une minoration de la différence

$\dim_m \mathcal{H}^I - \dim_m \mathcal{H}_{\bar{I}}$, nous avons dû faire certaines hypothèses. En l'absence d'hypothèse, nous n'avons pas su minorer cette différence.

Dans (VII) se trouvent un résumé de (VI) et l'essentiel du résultat démontré dans (IX).

Dans (VIII) nous essayons de généraliser la Δ -décomposition introduite par Iwasawa dans [9], en utilisant des définitions analogues à celles de (VI). Nous supposons toujours que L/k est une extension abélienne et que G est son groupe de Galois. Nous désignons ici par I un idéal de $\mathbb{Z}_{\ell}[G]$ et k_{∞}/k une $\mathbb{Z}_{\ell}$ -extension de k . Pour tout entier r , k_r est le sous-corps de k_{∞} tel que $[k_r : k] = \ell^r$. Soit

il l'entier tel que $k_i = k_\infty \cap L$ et soit H le groupe de Galois de L/k_i . On pose $I_0 = I \cap \mathbb{Z}_\ell[H]$. On définit K_I comme le corps intermédiaire entre L et k_i tel que le groupe de Galois de L/K_I soit l'ensemble des σ de H vérifiant la condition : $\sigma-1$ appartient à I_0 . Pour tout r , entier positif, on pose $K_{I,r} = k_{r+1} K_I$ et $K_{I,\infty} = \bigcup_{r \geq 0} K_{I,r}$. Nous obtenons ainsi une $\mathbb{Z}_\ell$ -extension $K_{I,\infty}/K_I$ et pour tout r , le ℓ -groupe $\mathcal{H}(K_{I,r})$ des classes d'idéaux de $K_{I,r}$ est un $\mathbb{Z}_\ell[H]$ -module. Soit $\mathcal{H}_r^I$ le plus grand quotient de $\mathcal{H}(K_{I,r})$ annulé par l'idéal I_0 . On déduit alors de la théorie d'Iwasawa la proposition suivante :

Proposition : Il existe deux entiers positifs μ_I et λ_I et un entier ν_I tel que pour n assez grand, l'ordre de $\mathcal{H}_r^I$ soit de la forme :

$$|\mathcal{H}_r^I| = \ell^{\mu_I \ell^r + \lambda_I r + \nu_I}.$$

Supposons maintenant que L contienne une racine primitive $\ell^{\text{ème}}$ de l'unité. L'application χ^{**} de G dans le groupe des unités de $\mathbb{Z}_\ell$ permet de définir une involution du miroir dans l'algèbre $\mathbb{Z}_\ell[G]$. Soit $\bar{I}$ l'image de I par cette involution. On peut de la même façon qu'avec I , attacher à $\bar{I}$ le corps $K_{\bar{I}}$, des groupes $\mathcal{H}_r^{\bar{I}}$ et les paramètres $\mu_{\bar{I}}$, $\lambda_{\bar{I}}$ et $\nu_{\bar{I}}$. On déduit alors de (VI) la proposition suivante qui généralise l'inégalité classique " $\lambda^+ \leq \lambda^-$ " donnée en [9] :

Proposition : On suppose que L contient une racine primitive $\ell^{\text{ème}}$ de l'unité et est abélien sur $\mathbb{Q}$. On suppose aussi que k_∞/k est la $\mathbb{Z}_\ell$ -extension cyclotomique de k et que K_I est réel. Alors on a : $\lambda_I \leq \lambda_{\bar{I}}$.

Dans (IX) le groupe des classes d'idéaux considéré est défini un peu différemment. On désigne encore par ℓ un nombre premier impair. Soient χ un caractère abélien réel de conducteur f , $\mathbb{Q}_\ell(\chi)$ le corps obtenu en ajoutant à $\mathbb{Q}_\ell$ les valeurs prises par χ et $\mathbb{Z}_\ell(\chi)$ l'anneau des entiers de ce corps. Notons K le corps correspondant à χ c'est-à-dire le sous-corps de $\mathbb{Q}^{(f)}$ défini par l'égalité : $\text{Gal}(\mathbb{Q}^{(f)}/K) = \text{Ker } \chi$. Soit σ un générateur de $G = \text{Gal}(K/\mathbb{Q})$ et P_χ le polynôme ℓ -adique cyclotomique ayant $\chi(\sigma)$ comme racine. L'anneau quotient $\mathbb{Z}_\ell[G]/P_\chi(\sigma)\mathbb{Z}_\ell[G]$ est isomorphe à $\mathbb{Z}_\ell(\chi)$.

Introduisons la ℓ -extension U/K abélienne, maximale, non ramifiée en dehors de ℓ . Le groupe de Galois $\text{Gal}(U/K)$ est un $\mathbb{Z}_\ell[G]$ -module et on sait que son sous- $\mathbb{Z}_\ell$ -module de torsion $\mathcal{C}$ est fini. Ce sous-module $\mathcal{C}$ est un $\mathbb{Z}_\ell[G]$ -module et on considère le quotient $\mathcal{H}(\chi) = \mathcal{C} / \mathcal{C}^{P_\chi(\sigma)}$. C'est le plus grand quotient de $\mathcal{C}$ annihilé par $P_\chi(\sigma)$. C'est donc un $\mathbb{Z}_\ell(\chi)$ -module.

Remarque : Lorsque l'ordre g de χ n'est pas une puissance de ℓ , on remarque que $\mathcal{H}(\chi)$ est isomorphe, en tant que $\mathbb{Z}_\ell[G]$ -module, au groupe de Galois $\text{Gal}(N/K)$, où N/K est l'extension abélienne, non ramifiée en dehors de ℓ , maximale telle que $N/\mathbb{Q}$ soit galoisienne et telle que $\text{Gal}(N/K)$ soit un $\mathbb{Z}_\ell[G]$ -module annihilé par $P_\chi(\sigma)$. C'est la raison pour laquelle $\mathcal{H}(\chi)$ est aussi appelé un groupe de classes d'idéaux de K .

Nous avons démontré dans (IX) le théorème suivant :

Théorème : Si g n'est pas une puissance de ℓ , alors $\mathcal{H}(\chi)$ est annihilé, en tant que $\mathbb{Z}_\ell^{(g)}$ -module, par $L_\ell(1, \chi)$, valeur en 1 de la fonction L ℓ -adique relative à χ .

Si g est une puissance de ℓ et si ζ_g est une racine primitive $g^{\text{ème}}$ de 1, alors $\mathcal{H}(\chi)$ est annihilé par $(1 - \zeta_g) L_\ell(1, \chi)$.

Nous avons ainsi généralisé le travail de G. Gras : [6], qui supposait : " ℓ ne divise pas g ". La démonstration de ce résultat repose d'une part sur le théorème d'annulation des classes d'idéaux relatives par l'idéal de Stickelberger, et d'autre part sur la Spiegelungsrelation. Notons $K^{(n)}$ le corps obtenu en ajoutant à K toutes les racines $n^{\text{ème}}$ de 1, n étant une puissance de ℓ . Soit G_n le groupe de Galois de $K^{(n)}/\mathbb{Q}$. On montre dans (IX) que l'image par l'involution du miroir de $A_n[G_n]$ du résidu modulo n d'un certain élément de l'idéal de Stickelberger de $K^{(n)}$ correspond, via l'application restriction de $A_n[G_n]$ à $A_n[G]$ et l'application canonique de $\mathbb{Z}_\ell[G]$ sur $\mathbb{Z}_\ell(\chi)$, au résidu modulo n de l'approximation ℓ -adique de $L_\ell(1, \chi)$ (ou de $(1 - \zeta_g) L_\ell(1, \chi)$) donnée dans [4] ou [11]. On en déduit, en utilisant le même procédé que dans les articles précédents, que, si n est assez grand, cette approximation annule $\mathcal{H}(\chi)$.

Ce résultat fournit donc une indication sur la structure de $\mathcal{C}$ en tant que $\mathbb{Z}_\ell[G]$ -module. Il est à rapprocher du calcul de l'ordre de $\mathcal{C}$, effectué par

J. Coates dans [2]. Ce calcul montre que l'ordre de $\mathcal{C}$ s'exprime simplement en fonction du produit des $L_{\ell}(1, \psi)$; ψ parcourant l'ensemble des caractères de K , différents de 1.

BIBLIOGRAPHIE

=====

- [1] J.V. ARMITAGE and A. FRÖHLICH, Class numbers and unit signatures, Mathematika, London, t. 14 (1967).
- [2] J. COATES, p -adic L -functions and Iwasawa's theory, Proceeding of Durham symposium (1975).
- [3] P. DAMEY et J.J. PAYAN, Existence et construction des extensions galoisiennes et non abéliennes de degré 8 d'un corps de caractéristique différente de 2, J. für die reine und ang. Math. 244 (1970).
- [4] J. FRESNEL, Nombres de Bernouilli et fonctions L p -adiques, Ann. Inst. Fourier, 17, 2 (1967).
- [5] G. GRAS, Sur les ℓ -classes d'idéaux dans les extensions cycliques relatives de degré premier ℓ , Ann. Inst. Fourier, 23 (1973).
- [6] G. GRAS, Annulation du groupe des ℓ -classes généralisées d'une extension abélienne réelle de degré premier à ℓ , Ann. Inst. Fourier, 29 (1979).
- [7] H. HASSE, Invariante Kennzeichnung relativ abelscher Zahlkörper mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers, Abh. Deutsche Akad. Wiss. Berlin (1947).
- [8] H. HAYASHI, Note on the class numbers of the quadratic number fields $\mathbb{Q}(\sqrt{-p})$, $\mathbb{Q}(\sqrt{2p})$, $\mathbb{Q}(\sqrt{-2p})$ with a prime number $p \equiv 1 \pmod{4}$, Memoirs of the Fac. gen. Ed., Kumamoto Univ., Series Sciences, 13 (1978).
- [9] K. IWASAWA, On the theory of cyclotomic fields, Annals of Math. 70, 3 (1959).

- [10] P. KAPLAN, Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique et réciprocité biquadratique, J. Math. Soc. Japan 25 (1973).
- [11] T. KUBOTA und H. W. LEOPOLDT, Eine p-adische Theorie der Zetawerte, Teil I, J. für die reine und ang. Math. 213 (1964).
- [12] H. LANG and R. SCHERTZ, Kongruenzen zwischen Klassenzahlen quadratischer Zahlkörper, J. of Number Theory 8 (1976).
- [13] H. W. LEOPOLDT, Zur Struktur der ℓ -Klassengruppe galoisscher Zahlkörper, J. für die reine und ang. Math. 199 (1958).
- [14] A. SCHOLZ, Über die Beziehung der Klassenzahlen quadratischer Körper zueinander, J. für die reine und ang. Math. 166 (1931).

SPIEGELUNGSSATZ .

Par Bernard ORIAT .

Nous exposons ci-après un " Spiegelungssatz " un peu plus général que celui de Leopoldt ;[6] . L'extension $L/\mathbb{Q}$ considérée par ce dernier est remplacée par une extension L/k . Soit ℓ un nombre premier . Les hypothèses : " ℓ ne divise pas $[L:\mathbb{Q}]$ et L contient une racine primitive $\ell^{\text{ème}}$ de l'unité " sont remplacées par " ℓ ne divise pas $[L:k]$ et L contient une racine primitive ℓ^n de l'unité " . Le résultat obtenu (théorème III) a la forme suivante :

Soit ϕ un caractère de $G = \text{Gal}(L/k)$, irréductible sur $\mathbb{Q}_\ell$ et soit $\bar{\phi}$ son reflet . Notons $\dim_m \mathcal{X}^\phi$ le m -rang de la ϕ -composante du ℓ -groupe des classes d'idéaux $\mathcal{X}$ de L , et $\dim_\ell \mathcal{E}^{\circ\phi}$ le ℓ -rang de la ϕ -composante du groupe $\mathcal{E}^\circ$ des ℓ -unités primaires de L .

Nous obtenons les inégalités :

$$\dim_m \mathcal{X}^{\bar{\phi}} - \dim_m \mathcal{X}^\phi \leq \dim_\ell \mathcal{E}^{\circ\phi} ,$$

pour toute puissance de ℓ , notée m et inférieure à ℓ^n .

Dans son principe , la démonstration reste semblable à celle de Leopoldt .

I

Relation du miroir.

Notations . Nous désignerons par :

L/k une extension finie galoisienne de corps de nombres ,

G son groupe de Galois ,

m un entier ,

ζ une racine primitive $m^{\text{ème}}$ de l'unité .

Nous supposons que L contient ζ . D'autre part, soit M un corps de nombres contenant L , tel que M/k soit galoisienne et M/L abélienne d'exposant divisant m . Comme L contient les racines $m^{\text{ème}}$ de 1, l'extension M/L est une extension de Kummer d'exposant divisant m . Nous désignerons par W son radical, c'est-à-dire :

$$W = \{ w ; w \in M^*, w^m \in L \}.$$

Définitions de trois structures de G -modules. Soit τ un élément de G et t un prolongement de τ à M .

Considérons le groupe de Galois de M/L , noté $\text{Gal}(M/L)$. Si u appartient à $\text{Gal}(M/L)$ la quantité $t^{-1}ut$ appartient à $\text{Gal}(M/L)$ et elle est indépendante du choix de t . En posant $u^\tau = t^{-1}ut$ on définit sur $\text{Gal}(M/L)$ une structure de G -module.

On note $\text{Gal}(M/L)^\wedge$ le groupe des homomorphismes de $\text{Gal}(M/L)$ dans le groupe multiplicatif de L , noté L^* . Comme M/L est d'exposant divisant m , et que L contient les racines $m^{\text{ème}}$ de 1, ce groupe est le groupe des caractères de degré 1 de $\text{Gal}(M/L)$. Si γ appartient à $\text{Gal}(M/L)^\wedge$, nous définissons γ^τ en posant : $\gamma^\tau(u) = \gamma(u^\tau)$, pour tout u de $\text{Gal}(M/L)$. On obtient ainsi une structure de G -module pour $\text{Gal}(M/L)^\wedge$. (En toute rigueur, $\text{Gal}(M/L)$ étant un G -module à droite, il faudrait noter $\text{Gal}(M/L)^\wedge$ comme un G -module à gauche).

Considérons le groupe W/L^* . Si w appartient à W et si u appartient à $\text{Gal}(M/L)$, w^{u-1} est une racine $m^{\text{ème}}$ de 1 et appartient donc à L . Il s'en suit que $w^t L^*$ est indépendant du choix de t . En posant : $(wL^*)^\tau = w^t L^*$, on définit sur W/L^* une structure de G -module.

Rappelons que la théorie de Kummer donne un isomorphisme canonique α entre les deux groupes W/L^* et $\text{Gal}(M/L)^\wedge$ ainsi défini : Si wL^* appartient à W/L^* , l'homomorphisme $\alpha(wL^*)$ de $\text{Gal}(M/L)$ dans L^* correspondant à wL^* est défini par : $\alpha(wL^*)(u) = w^{u-1}$, pour tout u de $\text{Gal}(M/L)$.

Première définition de χ^* . Pour tout τ de G , nous désignerons par $\chi^*(\tau)$, la classe résiduelle modulo m définie par : $\zeta^\tau = \zeta^{\chi^*(\tau)}$. Il est clair que $\chi^*(\tau)$ ne dépend pas du choix de la racine primitive

$m^{\text{ème}}$ de l'unité : ζ . De plus, $\chi^*(\tau)$ étant première à m , on peut considérer χ^* comme une application de G dans $(\mathbb{Z}/m\mathbb{Z})^*$. C'est un homomorphisme.

Théorème I. Les structures de G -module de W/L^* et $\text{Gal}(M/L)^\wedge$ sont liées par la relation : $(\alpha(wL^*))^\tau = \alpha((wL^*)^{\chi^*(\tau)\tau^{-1}})$, pour tout w de W et tout τ de $\text{Gal}(M/L)$.

Leopoldt appelle cette relation : "Spiegelungsrelation".

Démonstration. Soit u un élément de $\text{Gal}(M/L)$. Les notations τ et t ont toujours le même sens. Nous avons, d'après la définition de

$\alpha(wL^*)$: $\alpha(wL^*)(u^\tau)w = w^{u^\tau}$. D'autre part :

$w^{t^{-1}u} = \alpha(wL^{*\tau^{-1}})(u)w^{t^{-1}}$, d'où l'on déduit que w^{u^τ} peut aussi s'écrire

sous la forme : $w^{u^\tau} = w^{t^{-1}ut} = (\alpha(wL^{*\tau^{-1}})(u)w^{t^{-1}})^t = (\alpha(wL^{*\tau^{-1}})(u))^\tau w$.

Or $\alpha(wL^{*\tau^{-1}})(u)$ est une racine $m^{\text{ème}}$ de 1. Son image par τ est donc égale à sa puissance $\chi^*(\tau)^{\text{ème}}$ et nous avons :

$w^{u^\tau} = \alpha((wL^*)^{\chi^*(\tau)\tau^{-1}})(u)w$. D'où la relation annoncée.

II

Décomposition du ℓ -groupe des classes d'idéaux et du groupe des ℓ -unités d'une extension de degré premier à ℓ . Caractère du groupe des ℓ -unités.

Nous désignerons toujours par L/k une extension finie galoisienne de corps de nombres et par G son groupe de Galois. Soit ℓ un nombre premier ne divisant pas le degré $[L:k]$. Cette hypothèse assure la semi-simplicité de l'algèbre $F_\ell[G]$.

Rappels concernant les caractères ℓ -adiques de G . On trouvera dans [7] un exposé élémentaire sur les caractères ℓ -adiques d'un groupe abélien. Pour le cas général, nous renvoyons à [3] et [9].

Soit ϕ un caractère irréductible de G sur le corps ℓ -adique : $\mathbb{Q}_\ell$. (C'est la trace d'une représentation linéaire irréductible de G sur $\mathbb{Q}_\ell$). Ce caractère ϕ est une application de G dans $\mathbb{Z}_\ell$ et comme ℓ ne divise pas l'ordre de G , son résidu modulo ℓ est

un caractère irréductible de G sur $\mathbb{F}_\ell$. De plus, on obtient par ce moyen une bijection entre l'ensemble des caractères irréductibles de G sur $\mathbb{Q}_\ell$ et l'ensemble des caractères irréductibles de G sur $\mathbb{F}_\ell$. ([3] §76). C'est la raison pour laquelle nous noterons de la même façon ϕ et son résidu modulo ℓ .

Soit χ un caractère de G absolument irréductible, au dessus de ϕ . Soit $\mathbb{Q}_\ell(\chi)$ son corps des valeurs. Comme l'algèbre $\mathbb{Q}_\ell[G]$ est décomposée, ϕ sera la trace de χ dans l'extension $\mathbb{Q}_\ell(\chi)/\mathbb{Q}_\ell$. Soit 1_ϕ l'idempotent associé à ϕ . Il est donné par :

$$1_\phi = (\chi(1) / |G|) \sum_{\sigma \in G} \phi(\sigma^{-1}) \sigma. \text{ Il s'agit donc d'un élément de } \mathbb{Z}_\ell[G].$$

Si H est un $\mathbb{Z}_\ell[G]$ -module noté multiplicativement, nous appellerons ϕ -composante de H , le sous-module :

$$H^{1_\phi} = \{ h^{1_\phi} ; h \in H \}.$$

Nous le noterons simplement H^ϕ . On déduit des relations d'orthogonalité entre caractères, que H est le produit direct : $H = \prod H^\phi$, ϕ parcourant l'ensemble des caractères irréductibles de G sur $\mathbb{Q}_\ell$.

Lemme II. Si H est un $\mathbb{Z}_\ell[G]$ -module et si J est un sous $\mathbb{Z}_\ell[G]$ -module de H , la ϕ -composante de H/J est canoniquement isomorphe au quotient des ϕ -composantes de H et J . C'est-à-dire :

$$H^\phi/J^\phi \cong (H/J)^\phi$$

En effet : considérons l'application de H^ϕ dans $(H/J)^\phi$, qui associe à h appartenant à H^ϕ , sa classe modulo J . C'est un homomorphisme surjectif qui a pour noyau J^ϕ .

Définitions des symboles : $\dim_\ell$, $\dim_m$, $\dim_\phi$, $\dim_{\phi m}$. Soit H un $\mathbb{Z}_\ell[G]$ -module tel que $H^\ell = 1$. Il s'agit donc d'un $\mathbb{F}_\ell[G]$ -module. Nous noterons $\dim_\phi H$ le nombre de $\mathbb{F}_\ell[G]$ -modules simples de caractère ϕ qui interviennent dans une décomposition de H en produit direct de $\mathbb{F}_\ell[G]$ -modules simples. Cette quantité est liée à la dimension de H^ϕ en tant que $\mathbb{F}_\ell$ -espace vectoriel par : $\dim_\ell H^\phi = \phi(1) \dim_\phi H$.

Soit maintenant H un $\mathbb{Z}_\ell[G]$ -module quelconque et soit m une puissance de ℓ . On désignera par $\dim_m H$ le m -rang de H , c'est-à-dire : $\dim_m H = \dim_\ell H^{m/\ell} / H^m$. On posera également :

$$\dim_{\phi m} H = \dim_\phi H^{m/\ell} / H^m. \text{ On déduit du lemme ci-dessus la relation:}$$

$\phi(1) \dim_{\phi_m} H = \dim_m H^\phi$. En effet:

$$\phi(1) \dim_{\phi} H^{m/\ell} / H^m = \dim_{\ell} (H^{m/\ell} / H^m)^{\phi} = \dim_{\ell} (H^{\phi})^{m/\ell} / (H^{\phi})^m = \dim_m H^{\phi}.$$

Groupe des ℓ -classes d'idéaux. Soit K un corps intermédiaire entre k et L , tel que K/k soit galoisien. Soit U le groupe de Galois de L/K . Désignons par $\mathcal{H}_K$ (resp. $\mathcal{H}_L$) le ℓ -groupe des classes d'idéaux de K (resp. L). Notons j l'application de $\mathcal{H}_K$ dans $\mathcal{H}_L$ déduite de l'injection canonique du groupe des idéaux de K dans le groupe des idéaux de L .

Soit ϕ un caractère irréductible de G sur $\mathbb{Q}_{\ell}$. Rappelons que l'ensemble des éléments τ de G , tels que $\phi(\tau) = \phi(1)$ est le noyau de la représentation linéaire de G de caractère ϕ . Nous l'appellerons simplement le noyau de ϕ . Si ϕ_1 est un caractère de G/U , en composant ϕ_1 avec la surjection canonique π de G sur G/U , on obtient un caractère ϕ de G dont le noyau contient U . Si ϕ_1 est irréductible, alors ϕ est irréductible. On obtient ainsi une bijection canonique entre l'ensemble des caractères irréductibles de G sur $\mathbb{Q}_{\ell}$ dont le noyau contient U et l'ensemble des caractères irréductibles de G/U sur $\mathbb{Q}_{\ell}$. Désignons encore par π l'application de $\mathbb{Q}_{\ell}[G]$ sur $\mathbb{Q}_{\ell}[G/U]$ déduite de π par linéarité. Si $\phi = \phi_1 \circ \pi$, les idempotents associés à ϕ et ϕ_1 vérifient : $\pi(1_{\phi}) = 1_{\phi_1}$.

Proposition II a. L'application j est un homomorphisme injectif. Son image $j(\mathcal{H}_K)$ est l'ensemble des éléments de $\mathcal{H}_L$ invariants par $U = \text{Gal}(L/K)$. Si ϕ_1 est un caractère de G/U irréductible sur $\mathbb{Q}_{\ell}$ et si $\phi = \phi_1 \circ \pi$, on a alors : $j(\mathcal{H}_K^{\phi_1}) = \mathcal{H}_L^{\phi}$.

Démonstration. Désignons par A_K , A_L les anneaux d'entiers de K et L . Soit $\mathfrak{a}$ un idéal de K dont la classe appartient à $\text{Ker } j$. Il existe donc a dans L tel que : $\mathfrak{a}A_L = aA_L$, d'où :
 $\mathfrak{a}^{[L:K]} = N_{L/K}(a) A_K$ et $\mathfrak{a}^{[L:K]}$ est principal. Or $\text{Cl}_K(a)$ est

d'ordre une puissance de ℓ et ℓ ne divise pas $[L:K]$. L'idéal α est donc principal et j est injectif.

Soit α un idéal de L , dont la classe est invariante par U . On aura alors $N_{L/K}(\alpha) A_L = \alpha^{[L:K]}$. En utilisant une relation de Bezout entre $[L:K]$ et l'ordre de $\text{Cl}_L(\alpha)$, on obtient :
 $\text{Cl}_L(\alpha) = \text{Cl}_L(N_{L/K}(\alpha)^u A_L)$ et cela montre que $\text{Cl}_L(\alpha)$ appartient à $j(\mathcal{H}_K)$. Comme $\prod(1_\phi) = 1_{\phi_1}$, nous avons $\mathcal{H}_K^{1_{\phi_1}} = \mathcal{H}_K^{1_\phi}$ et
 $j(\mathcal{H}_K^{\phi_1}) = j(\mathcal{H}_K)^\phi \subset \mathcal{H}_L^\phi$. Réciproquement, si τ appartient à U , τ appartient à $\text{Ker } \phi$ et vérifie : $\tau 1_\phi = 1_\phi$. On en déduit que tout élément de $\mathcal{H}_L^\phi$ est invariant par U , ce qui démontre l'inclusion :
 $\mathcal{H}_L^\phi \subset j(\mathcal{H}_K^{\phi_1})$.

Conséquence. Convenons d'identifier l'ensemble des caractères de G/U irréductibles sur $\mathbb{Q}_\ell$ à l'ensemble des caractères de G , irréductibles sur $\mathbb{Q}_\ell$ et dont le noyau contient U . Convenons également de considérer $\mathcal{H}_K$ comme un sous-groupe de $\mathcal{H}_L$. Nous constatons alors que la décomposition du ℓ -groupe des classes de tout corps intermédiaire K galoisien sur k , pourra s'écrire : $\mathcal{H}_K = \prod_{\phi} \mathcal{H}_L^\phi$, ce produit étant direct et étendu aux caractères irréductibles sur $\mathbb{Q}_\ell$ de $G/U = \text{Gal}(K/k)$.

Groupe des ℓ -unités. On désigne encore par K un corps intermédiaire entre L et k , galoisien sur k et par U le groupe de Galois : $\text{Gal}(L/K)$. Soit E_K le groupe des unités de K . Posons :
 $\mathcal{E}_K = E_K / E_K^\ell$. Nous appellerons $\mathcal{E}_K$ le groupe des ℓ -unités de K . Nous désignerons par i l'application de $\mathcal{E}_K$ dans $\mathcal{E}_L$ déduite de l'injection canonique de E_K dans E_L .

Proposition II b. L'application i est un homomorphisme injectif. Son image $i(\mathcal{E}_K)$ est l'ensemble des éléments de $\mathcal{E}_L$ invariants par $U = \text{Gal}(L/K)$. Si ϕ_1 est un caractère de G/U irréductible sur

$\mathbb{Q}_\ell$ et si $\phi = \phi_1 \circ \pi$, alors $i(\mathcal{E}_K^{\phi_1}) = \mathcal{E}_L^\phi$.

La démonstration de cette proposition est semblable à celle de la proposition précédente.

Deuxième définition de χ^* . Soit T le sous-groupe de torsion de E_L . Considérons le quotient T/T^ℓ . C'est un $\mathbb{F}_\ell[G]$ -module. Il n'est pas réduit à 1 si et seulement si L contient une racine primitive $\ell^{\text{ème}}$ de 1. Supposons que cette condition soit vérifiée et appelons ζ une racine de 1 appartenant à L , d'ordre une puissance de ℓ la plus grande possible : ℓ^n . La classe de ζ modulo T^ℓ engendre donc T/T^ℓ . Introduisons l'application χ^* définie au paragraphe précédent comme un homomorphisme de G dans $(\mathbb{Z}/\ell^n\mathbb{Z})^*$ tel que : $\zeta^\sigma = \zeta^{\chi^*(\sigma)}$. Considérons le résidu modulo ℓ de χ^* , c'est-à-dire l'application de G dans $(\mathbb{Z}/\ell\mathbb{Z})^*$ qui associe à σ la classe de $\chi^*(\sigma)$ modulo ℓ . Il s'agit du caractère du $\mathbb{F}_\ell[G]$ -module T/T^ℓ . Nous appellerons ce caractère le miroir de L/k et nous le noterons encore χ^* . Par la suite, comme nous l'avons dit au début de ce paragraphe, nous désignerons aussi par χ^* le caractère de G sur $\mathbb{Q}_\ell$ dont il est le résidu modulo ℓ . En ce sens, χ^* est l'homomorphisme de G dans le groupe multiplicatif de $\mathbb{Z}_\ell$ tel que $\zeta^\sigma = \zeta^{\chi^*(\sigma)}$ pour tout σ de G .

Nous allons essayer maintenant d'exprimer le caractère du $\mathbb{F}_\ell[G]$ -module $\mathcal{E}_L$.

Définition de ψ_0 . Désignons par σ_∞ la conjugaison complexe de $\mathbb{C}$. Soient $\pi_1, \dots, \pi_s$ les plongements réels de L dans $\mathbb{C}$ et $\pi_{1+s}, \dots, \pi_{t+s}$, $\bar{\pi}_{1+s}, \dots, \bar{\pi}_{t+s}$ les plongements complexes de L dans $\mathbb{C}$. Convenons que $\bar{\pi}$ est le conjugué de π , c'est-à-dire que $\bar{\pi} = \pi \sigma_\infty$. Nous définissons ψ_0 de la façon suivante : si τ appartient à G et diffère de 1, alors $\psi_0(\tau)$ est le demi nombre de plongements complexes π de L dans $\mathbb{C}$ tels que $\bar{\pi} = \tau \pi$. D'autre part, on posera $\psi_0(1) = s+t$.

Cas particulier. Supposons un instant $L/\mathbb{Q}$ galoisienne. Supposons L plongé dans $\mathbb{C}$ et soit $L_0 = L \cap \mathbb{R}$ et $H_0 = \text{Gal}(L/L_0)$. Le groupe H_0

possède donc 1 ou 2 éléments . On peut alors vérifier que l'application Ψ_0 définie ci-dessus est la restriction à G du caractère de $\text{Gal}(L/\mathbb{Q})$ induit par le caractère principal de H_0 .

Théorème II . Soit L/k une extension finie galoisienne , de groupe de Galois G . Soit ℓ un nombre premier ne divisant pas $[L:k]$. Soit $\mathcal{E}_L$ le groupe des ℓ -unités de L , c'est-à-dire : $\mathcal{E}_L = E_L / E_L^\ell$. Notons 1 le caractère unité de G . Si L contient une racine primitive $\ell^{\text{ème}}$ de l'unité , alors le caractère du $\mathbb{F}_\ell[G]$ -module $\mathcal{E}_L$ est $\Psi_L = \chi_+^* \Psi_0^{-1}$. Si L ne contient pas de racine primitive $\ell^{\text{ème}}$ de l'unité , le caractère de $\mathcal{E}_L$ est $\Psi_L = \Psi_0^{-1}$.

Corollaire . Soit ϕ un caractère de G , irréductible sur $\mathbb{Q}_\ell$. Soit χ le caractère absolument irréductible dont ϕ est issu . Le nombre de modules simples de caractères ϕ dont $\mathcal{E}_L$ est produit direct est : $\dim_\phi \mathcal{E}_L = (1/|G|) \sum_{\sigma \in G} \chi(\sigma^{-1}) \Psi_L(\sigma)$.

Démonstration . Soit $\mathcal{L} : \begin{matrix} E_L & \longrightarrow & \mathbb{R}^{t+s} \\ \varepsilon & \longrightarrow & (\text{Log} |\varepsilon^{\prod_i}|)_{1 \leq i \leq s+t} \end{matrix}$

le plongement canonique de E_L dans $\mathbb{R}^{s+t}$. Rappelons que $\mathcal{L}(E_L)$ est un sous-groupe discret de l'hyperplan de $\mathbb{R}^{s+t}$ d'équation : $\sum x_i + 2 \sum x_{s+i} = 0$. Définissons sur $\mathbb{R}^{s+t}$ une structure de G -module de la façon suivante : Si τ appartient à G , soit j_τ l'application de l'ensemble des $s+t$ premiers nombres entiers dans lui-même , définie par $\tau \prod_i = \prod_{j_\tau(i)} \text{ ou } \overline{\prod_{j_\tau(i)}}$. Soit $(x_i)_{1 \leq i \leq s+t}$ un élément de $\mathbb{R}^{s+t}$. Faisons opérer (à droite) G sur $\mathbb{R}^{s+t}$ en posant :

$(x_i)_{1 \leq i \leq s+t} \cdot \tau = (x_{j_\tau(i)})_{1 \leq i \leq s+t}$. Le plongement $\mathcal{L}$ devient alors un homomorphisme de G -modules .

Soit D le sous-ensemble de $\mathbb{R}^{s+t}$ ainsi défini :

$D = \{(\lambda, \dots, \lambda) ; \lambda \in \mathbb{Z}\}$. La somme directe $\mathcal{L}(E_L) \oplus D$ est un sous-

groupe discret de $\mathbb{R}^{s+t}$. Il s'en suit, qu'une $\mathbb{Z}$ -base de $\mathcal{L}(E_L) \oplus D$ sera une $\mathbb{R}$ -base de $\mathbb{R}^{s+t}$. Si τ appartient à G , soit A_τ la matrice de l'application de $\mathcal{L}(E_L) \oplus D$ dans lui-même qui associe à

$$\left(x_i \right)_{1 \leq i \leq s+t}, \left(x_i \right) \cdot \tau_{1 \leq i \leq s+t}. \text{ L'application qui associe à } \tau, \text{ la trace de}$$

A_τ est le caractère du $\mathbb{Q}[G]$ -module $(\mathcal{L}(E_L) \oplus D) \cdot \mathbb{Q}$, c'est-à-dire du $\mathbb{Q}[G]$ -module déduit de $\mathcal{L}(E_L) \oplus D$ par extension de l'anneau des scalaires à $\mathbb{Q}[G]$. Le résidu modulo ℓ de cette application sera le caractère du $\mathbb{F}_\ell[G]$ -module $\mathcal{L}(E_L) \oplus D / \ell(\mathcal{L}(E_L) \oplus D)$.

Pour calculer $\text{Tr}(A_\tau)$, il suffit de chercher comment A_τ transforme la base canonique de $\mathbb{R}^{s+t}$. On obtiendra : $\text{Tr}(A_1) = s+t$, Si τ diffère de 1, la trace de A_τ est le nombre des entiers i compris entre $s+1$ et $s+t$ tels que $i\tau(i) = i$. L'application: $\tau \longrightarrow \text{Tr}(A_\tau)$, est donc égale à Ψ_0 .

Comme G agit trivialement sur D , on en déduit que $\Psi_0 - 1$ est le caractère de $\mathcal{L}(E_L) \cdot \mathbb{Q}$, c'est-à-dire du $\mathbb{Q}[G]$ -module déduit de $\mathcal{L}(E_L)$ par extension de l'anneau des scalaires à $\mathbb{Q}[G]$. Le résidu modulo ℓ de $\Psi_0 - 1$ sera le caractère du $\mathbb{F}_\ell[G]$ -module $\mathcal{L}(E_L) / \ell \mathcal{L}(E_L)$. De plus, le noyau de $\mathcal{L}$ est le sous-groupe de torsion T de E_L et $\mathcal{L}(E_L) / \ell \mathcal{L}(E_L)$ est quotient de $E_L / E_L^\ell = \mathcal{E}_L$ par T / T^ℓ . Il s'en suit, que le caractère de $\mathcal{E}_L$, Ψ_L , est obtenu en ajoutant à $\Psi_0 - 1$, le caractère de T / T^ℓ . Si ce groupe est réduit à 1, c'est-à-dire si L ne contient pas de racine primitive $\ell^{\text{ème}}$ de 1, son caractère est nul; sinon, il s'agit du miroir: χ^* .

Le corollaire s'en déduit. En effet le produit scalaire de χ et Ψ_L : $(1 / |G|) \sum_{\sigma \in G} \chi(\sigma^{-1}) \Psi_L(\sigma)$ mesure le nombre de modules simples de caractères ϕ dont $\mathcal{E}_L$ est produit direct.

III

Enoncé du Spiegelungssatz .

Nous désignerons toujours par L/k une extension finie galoisienne de corps de nombres , par G son groupe de Galois , par ℓ un nombre premier .

Hypothèses . On suppose que L contient une racine primitive ζ d'ordre ℓ^n de 1 et que $[L:k]$ est premier à ℓ .

Définitions . Rappelons d'abord que χ^* , appelé le miroir de L/k , est le caractère de G sur $\mathbb{Q}_\ell$ défini par $\chi^* = \chi^{\chi^*(\sigma)}$ pour tout σ de G . Si ϕ est un caractère irréductible de G sur $\mathbb{Q}_\ell$, nous poserons : $\bar{\phi}(\tau) = \phi(\tau^{-1}) \chi^*(\tau)$, pour tout τ de G . En introduisant la représentation dont ϕ est le caractère, on vérifie que $\bar{\phi}$ est le caractère d'une représentation linéaire de G sur $\mathbb{Q}_\ell$. Ce caractère $\bar{\phi}$ est aussi irréductible sur $\mathbb{Q}_\ell$. On l'appellera le "reflet" de ϕ . (Spiegelbild). L'application $\phi \rightarrow \bar{\phi}$ est une involution de l'ensemble des caractères irréductibles de G sur $\mathbb{Q}_\ell$; c'est-à-dire : $\bar{\bar{\phi}} = \phi$.

Soit E (resp. E°) le groupe des unités de L (resp. des unités ℓ -primaires de L). On pose $\mathcal{E} = E/E^\ell$ et $\mathcal{E}^\circ = E^\circ/E^\ell$. On appelle ces groupes : groupes des ℓ -unités de L et groupes des ℓ -unités primaires de L .

Les symboles $\dim_{\phi_m}$ et $\dim_\phi$ ont été définis au paragraphe précédent .

Théorème III Soient L/k une extension finie galoisienne de corps de nombres et G son groupe de Galois . Soit ℓ un nombre premier . On suppose que L contient une racine ℓ^n ème de 1 et que ℓ ne divise pas le degré $[L:k]$. Pour toute puissance de ℓ , notée m , et inférieure à ℓ^n , et pour tout caractère ϕ de G irréductible sur $\mathbb{Q}_\ell$, les ϕ et $\bar{\phi}$ -composantes du ℓ -groupe des classes $\mathcal{H}$ de L et la ϕ -composante du groupe des ℓ -unités primaires de L vérifient :

$$\dim_{\bar{\phi}_m} \mathcal{H} - \dim_{\phi_m} \mathcal{H} \leq \dim_\phi \mathcal{E}^\circ .$$

Remarque . Comme $\mathcal{E}^\circ$ s'injecte dans $\mathcal{E}$, nous avons aussi :
 $\dim_\phi \mathcal{E}^\circ \leq \dim_\phi \mathcal{E}$. Cette dernière valeur est donnée par le théorème II.

IV

Démonstration du théorème III .

Lemme IV . Soit H un $\mathbb{Z}_\ell[G]$ -module et $H^\wedge$ son dual , c'est-à-dire le groupe des homomorphismes de H dans $\mathbb{C}^*$. Munissons $H^\wedge$ de la structure de $\mathbb{Z}_\ell[G]$ -module ainsi définie : $\gamma^\tau(x) = \gamma(x^\tau)$, pour tout τ de G et tout x de H . Pour tout caractère ϕ de G irréductible sur $\mathbb{Q}_\ell$, les modules $(H^\phi)^\wedge$ et $(H^\wedge)^\phi$ sont canoniquement isomorphes .

Démontrons ce lemme . Considérons l'application de $(H^\wedge)^\phi$ dans $(H^\phi)^\wedge$ qui associe à γ , appartenant à $(H^\wedge)^\phi$, sa restriction à H^ϕ . C'est un homomorphisme . Montrons qu'il est injectif .
 Supposons que la restriction de γ à H^ϕ soit égale à 1 . Pour tout x de H et pour tout caractère ψ de G irréductible sur $\mathbb{Q}_\ell$ et différent de ϕ , nous avons : $\gamma(x^{1\psi}) = \gamma(x^{1\phi 1\psi}) = \gamma(1) = 1$. D'où l'on déduit que : $\gamma(x^{1\psi}) = 1$ pour tout caractère ψ ; d'où finalement : $\gamma = 1$. Pour montrer que cet homomorphisme est surjectif , considérons un élément δ de $(H^\phi)^\wedge$. Comme H est égal au produit direct : $H = \prod H^\psi$, ψ parcourant l'ensemble des caractères irréductibles de G sur $\mathbb{Q}_\ell$, il est possible d'obtenir un prolongement γ de δ à H tel que la restriction de γ à H^ψ , pour tout ψ différent de ϕ , soit égale à 1 .

Venons en à la démonstration proprement dite du théorème III .
 Désignons par M/L la ℓ -extension abélienne non ramifiée maximale de L . Pour tout m , puissance de ℓ inférieure à ℓ^n , désignons par M_m le corps intermédiaire entre M et L maximal tel que M_m/L soit d'exposant divisant m . L'extension M_m/L est une extension de Kummer et l'on désigne par W_m son radical ; c'est à-dire :

$$W_m = \{ w ; w \in M_m ; w^m \in L^* \} . \text{ (On a donc : } M_1 = L \text{ et } W_1 = L^* \text{)} .$$

Munissons W_m/L^* , $\text{Gal}(M_m/L)$ et $\text{Gal}(M_m/L)^\wedge$ des structures de G -modules définies au paragraphe I . Rappelons que $\mathcal{H}$ et

$\text{Gal}(M/L)$ sont isomorphes (en tant que G -modules) par l'isomorphisme de réciprocité du corps des classes . Les groupes $\text{Gal}(M/M_m)$ et $\text{Gal}(M/M_{m/\ell})$ correspondent dans cet isomorphisme à $\mathcal{H}^m$ et $\mathcal{H}^{m/\ell}$. Par restriction et passage au quotient , on en déduit l'existence d'un isomorphisme de G -modules entre : $\text{Gal}(M_m/M_{m/\ell})$ et $\mathcal{H}^{m/\ell}/\mathcal{H}^m$. D'où l'égalité :

$$\dim_{\bar{\phi}_m} \mathcal{H} = \dim_{\bar{\phi}} \mathcal{H}^{m/\ell} / \mathcal{H}^m = \dim_{\bar{\phi}} \text{Gal}(M_m/M_{m/\ell}) .$$

D'autre part , $W_{m/\ell}/L^*$ est un sous- G -module de W_m/L^* et nous confondrons le quotient $(W_m/L^*)/(W_{m/\ell}/L^*)$ avec $W_m/W_{m/\ell}$ qui lui est canoniquement isomorphe . L'isomorphisme de la théorie de Kummer $\alpha_m : W_m/L^* \cong \text{Gal}(M_m/L)^\wedge$ a pour restriction à $W_{m/\ell}/L^*$ l'isomorphisme $\alpha_{m/\ell} : W_{m/\ell}/L^* \cong \text{Gal}(M_{m/\ell}/L)^\wedge$. En effectuant le quotient , on obtient un isomorphisme de groupes :

$$\beta_m : W_m/W_{m/\ell} \cong \text{Gal}(M_m/M_{m/\ell})^\wedge .$$

Nous avons vu (Théorème I) que la relation du miroir était :

$$(\alpha_m(wL^*))^\tau = \alpha_m((wL^*)^{\chi^*(\tau)\tau^{-1}}) .$$

Maintenant , ℓ ne divise pas l'ordre de G et on en déduit :

$$(\alpha_m(wL^*))^{1\phi} = \alpha_m((wL^*)^{1\bar{\phi}}) .$$

En passant au quotient , on obtient :

$$(\beta_m(wW_{m/\ell}))^{1\phi} = \beta_m((wW_{m/\ell})^{1\bar{\phi}}) , \text{ pour tout } w \text{ de } W_m .$$

Dans l'isomorphisme β_m , $\text{Gal}(M_m/M_{m/\ell})^\wedge \bar{\phi}$ correspond donc à $(W_m/W_{m/\ell})^\phi$. D'après le lemme IV , $\text{Gal}(M_m/M_{m/\ell})^\wedge \bar{\phi}$ est un groupe isomorphe à $\text{Gal}(M_m/M_{m/\ell})^{\bar{\phi}^\wedge}$. Nous aurons donc :

$\dim_{\ell} \text{Gal}(M_m/M_{m/\ell})^{\bar{\phi}} = \dim_{\ell} (W_m/W_{m/\ell})^\phi$. Comme $\phi(1) = \bar{\phi}(1)$, nous en déduisons : $\dim_{\bar{\phi}} \text{Gal}(M_m/M_{m/\ell}) = \dim_{\phi} W_m/W_{m/\ell}$. Nous avons démontré :

Proposition IV a . Les quantités : $\dim_{\bar{\phi}_m} \mathcal{H}$ et $\dim_{\phi} W_m/W_{m/\ell}$ sont égales .

Définitions des applications θ_m et ψ_m . Notons $\mathcal{H}^{(m)}$ l'ensemble des éléments de $\mathcal{H}$ dont la puissance $m^{\text{ème}}$ est égale à 1. C'est-à-dire : $\mathcal{H}^{(m)} = \{h ; h \in \mathcal{H} ; h^m = 1\}$. Notons A_L l'anneau des entiers de L . Si w appartient à W_m , sa puissance $m^{\text{ème}}$ appartient à L et engendre un idéal qui est une puissance $m^{\text{ème}}$ d'un idéal α de L . On a donc : $w^m A_L = \alpha^m$. La classe de l'idéal α (notée $Cl(\alpha)$) est un élément de $\mathcal{H}^{(m)}$. En associant à $wW_{m/\ell}$ la classe de $Cl(\alpha)$ modulo $\mathcal{H}^{(m/\ell)}$, on définit une application :

$$\theta_m : W_m / W_{m/\ell} \longrightarrow \mathcal{H}^{(m)} / \mathcal{H}^{(m/\ell)}.$$

Il s'agit d'un homomorphisme de G -modules.

Soit $wW_{m/\ell}$ un élément du noyau de θ_m . Si $w^m A_L = \alpha^m$, il existe donc un élément a de L tel que $\alpha^{m/\ell} = a A_L$. D'où $w^m A_L = a^\ell A_L$ et il existe une unité ε de L telle que $w^m = a^\ell \varepsilon$. L'extension $L(\sqrt[\ell]{\varepsilon})/L$ est une sous-extension de M_m/L et elle est donc non ramifiée. L'unité ε est donc ℓ -primaire et appartient à E° . Soit

$$\psi_m : \text{Ker } \theta_m \longrightarrow \mathcal{E}^\circ$$

l'application de $\text{Ker } \theta_m$ dans $E^\circ/E^\ell = \mathcal{E}^\circ$ qui associe à $w^m W_{m/\ell}$ la classe de ε modulo E^ℓ . On vérifie que ψ_m est un homomorphisme de G -modules. De plus ψ_m est injectif. En effet si ε appartient à E^ℓ , w^m appartient à L^ℓ et $w^{m/\ell}$ appartient à L . D'où w appartient à $W_{m/\ell}$. Nous avons démontré :

Proposition IV b. Il existe un homomorphisme de G -modules θ_m de $W_m / W_{m/\ell}$ dans $\mathcal{H}^{(m)} / \mathcal{H}^{(m/\ell)}$. Il existe un homomorphisme de G -modules, injectif ψ_m de $\text{Ker } \theta_m$ dans $\mathcal{E}^\circ$. On en déduit les inégalités :

$$\dim_{\phi} W_m / W_{m/\ell} - \dim_{\phi} \mathcal{H}^{(m)} / \mathcal{H}^{(m/\ell)} \leq \dim_{\phi} \text{Ker } \theta_m \leq \dim_{\phi} \mathcal{E}^\circ.$$

Pour déduire le théorème III de ces deux propositions, il reste à voir que $\dim_{\phi} \mathcal{H}^{(m)} / \mathcal{H}^{(m/\ell)} = \dim_{\phi_m} \mathcal{H}$. Or nous avons d'après le lemme II : $(\mathcal{H}^{m/\ell} / \mathcal{H}^m)^{\phi} \cong \mathcal{H}^{\phi m/\ell} / \mathcal{H}^{\phi m}$. Ce groupe est isomorphe en tant que $\mathbb{F}_\ell$ -module à $\mathcal{H}^{\phi(m)} / \mathcal{H}^{\phi(m/\ell)}$ et celui-ci est isomorphe,

d'après le lemme II à : $(\mathcal{H}^{(m)} / \mathcal{H}^{(m/\ell)})^\phi$. Nous avons donc :
 $\dim_\ell (\mathcal{H}^{m/\ell} / \mathcal{H}^m)^\phi = \dim_\ell (\mathcal{H}^{(m)} / \mathcal{H}^{(m/\ell)})^\phi$. En multipliant par $\phi(1)$,
 nous obtenons : $\dim_\phi \mathcal{H}^{m/\ell} / \mathcal{H}^m = \dim_\phi \mathcal{H}^{(m)} / \mathcal{H}^{(m/\ell)}$.

V

Exemples .

1. Rappels concernant les classes réelles et les classes relatives .

Soit L/k une extension finie de corps de nombres ; soient $\tilde{L}$ et $\tilde{k}$ les corps des classes de Hilbert de L et k , et soient H_k et H_L les groupes des classes d'idéaux de k et L . Désignons par N l'application de H_L dans H_k déduite de la norme dans l'extension L/k .

Proposition V a . Dans l'isomorphisme de réciprocité liant H_k et $\text{Gal}(\tilde{k}/k)$, l'image de H_L par N correspond à $\text{Gal}(\tilde{k}/L\tilde{k})$. Dans l'isomorphisme de réciprocité liant H_L et $\text{Gal}(\tilde{L}/L)$ le noyau de N correspond à $\text{Gal}(\tilde{L}/L\tilde{k})$.

Démonstration. Si $\mathfrak{b}$ est un idéal de L , le symbole d'Artin : $(N_{L/k}(\mathfrak{b}), \tilde{k}/k)$ est la restriction à $\tilde{k}$ de $(\mathfrak{b}, L\tilde{k}/L)$ et il laisse invariant $\tilde{k} \cap L$. Donc il appartient à $\text{Gal}(\tilde{k} / \tilde{k} \cap L)$. Réciproquement, soit σ un élément de $\text{Gal}(\tilde{k} / \tilde{k} \cap L)$. Cet automorphisme est la restriction à $\tilde{k}$ d'un automorphisme τ de $L\tilde{k}/L$ et il existe un idéal $\mathfrak{b}$ de L tel que $\tau = (\mathfrak{b}, L\tilde{k}/L)$; d'où : $\sigma = (N_{L/k}(\mathfrak{b}), \tilde{k}/k)$. La deuxième assertion se démontre de la même façon.

Définitions . Soit L un corps de nombres plongé dans $\mathbb{C}$. Posons $L_\circ = L \cap \mathbb{R}$. On appelle groupe des classes réelles de L , le groupe des classes de $L_\circ$ et on appelle groupe des classes relatives de L , le noyau de l'application N de H_L dans $H_{L_\circ}$ déduite de la norme relative à $L/L_\circ$. (Ces notions dépendent donc du plongement de L dans $\mathbb{C}$ choisi. Si $L/\mathbb{Q}$ est abélienne, $L_\circ$ ne dépend plus de ce plongement)

On déduit de la proposition ci-dessus que l'application N est surjective . En effet , puisqu'aucune place de L ne peut se ramifier dans le corps des classes de Hilbert $\tilde{L}_0$ de L_0 , l'intersection $\tilde{L}_0 \cap L$ sera égale à L_0 . Il s'en suit que $N(H_L) = H_{L_0}$. Nous avons démontré :

Corollaire . Le groupe des classes réelles de L est isomorphe au quotient du groupe des classes de L par le groupe des classes relatives de L .

2. Comparaison du ℓ -groupe des classes relatives et du ℓ -groupe des classes réelles de L , lorsque L contient une racine $\ell^{\text{ème}}$ de 1 et lorsque $[L:L_0] = 2$.

Désignons encore par L un corps de nombres plongé dans $\mathbb{C}$ et par L_0 l'intersection : $L_0 = L \cap \mathbb{R}$. L'extension L/L_0 est galoisienne si et seulement si $[L:L_0] \leq 2$. En effet , si L/L_0 est galoisienne , de degré différent de 1 , la restriction ^{σ_∞} de la conjugaison de $\mathbb{C}$ à L appartient au groupe de Galois de L/L_0 . Le corps fixe de σ_∞ sera donc L_0 et $[L:L_0] = 2$.

Supposons désormais , que L (et son plongement dans $\mathbb{C}$) vérifie cette condition . Soit ℓ un nombre premier impair et soit $\mathcal{H}$ (resp. $\mathcal{H}_0$, $\mathcal{H}^*$) le ℓ -Sylow du groupe des classes de L (resp. du groupe des classes réelles de L , du groupe des classes relatives de L) . D'après le corollaire énoncé ci-dessus , nous avons : $\mathcal{H}_0 \cong \mathcal{H} / \mathcal{H}^*$. Mais nous pouvons énoncer un résultat plus précis : $\mathcal{H}$ est produit direct de $\mathcal{H}_0$ et $\mathcal{H}^*$.

En effet , supposons $[L:L_0] = 2$. (Sinon , c'est clair) . Posons : $L_0 = k$, $G = \text{Gal}(L/k) = \{1, \sigma_\infty\}$. Le groupe G possède deux caractères irréductibles sur $\mathbb{Q}_\ell$: 1 et ϕ donnés par le tableau :

	1	σ_∞
1	1	1
ϕ	1	-1

Les idempotents correspondants sont : $1_1 = \frac{1}{2} (1 + \sigma_\infty)$ et $1_\phi = \frac{1}{2} (1 - \sigma_\infty)$.

D'après la proposition II a (appliquée avec $K = k = L_o$) le groupe $\mathcal{H}^1$ est isomorphe par l'injection j de $\mathcal{H}_o$ dans $\mathcal{H}$, au ℓ -groupe des classes réelles $\mathcal{H}_o$ de L . On vérifie aussi, que $\mathcal{H}^\phi$ coïncide avec le ℓ -groupe $\mathcal{H}^*$ des classes relatives de L . Enfin, il est clair que $\mathcal{H}$ est produit direct de $\mathcal{H}^1$ et $\mathcal{H}^\phi$.

La proposition suivante a été obtenue par L. Bouvier dans [2] sous des hypothèses un peu plus restrictives :

Proposition V b. Soit L un corps de nombres plongé dans $\mathbb{C}$ et soit $L_o = L \cap \mathbb{R}$. On suppose que $[L:L_o] = 2$. Si ℓ est un nombre premier impair, soit n le plus grand entier tel que L contienne une racine ℓ^n ème de 1, notée ζ . Supposons $n \neq 0$. (C'est -à-dire : supposons que L contienne une racine primitive $\ell^{\text{ème}}$ de 1) Pour toute puissance de ℓ , notée m et inférieure à ℓ^n , les m -rangs des ℓ -groupes des classes réelles et relatives : $\mathcal{H}_o$ et $\mathcal{H}^*$ de L , vérifient les inégalités :

$$\begin{aligned} \dim_m \mathcal{H}^* - \dim_m \mathcal{H}_o &\leq \dim_{\mathbb{Z}} E_L, \\ \dim_m \mathcal{H}_o - \dim_m \mathcal{H}^* &\leq \dim_{\mathbb{Z}} E_L - \dim_{\mathbb{Z}} E_{L_o} + 1. \end{aligned}$$

Si de plus, ζ n'est pas une unité ℓ -primaire de L , on a alors plus précisément :

$$\dim_m \mathcal{H}_o - \dim_m \mathcal{H}^* \leq \dim_{\mathbb{Z}} E_L - \dim_{\mathbb{Z}} E_{L_o}.$$

Les quantités $\dim_{\mathbb{Z}} E_L$ et $\dim_{\mathbb{Z}} E_{L_o}$ sont les dimensions des $\mathbb{Z}$ -modules libres, quotients des groupes des unités E_L et E_{L_o} de L et L_o par leurs sous-groupes de torsion.

Démonstration. Appliquons le théorème III à L et $k = L_o$. Comme $\zeta^{\mathbb{Q}} = \zeta^{-1}$, le caractère miroir de L/k est ϕ . De plus 1 et ϕ sont reflètes l'un de l'autre. Nous avons donc :

$$\begin{aligned} \dim_{1m} \mathcal{H} - \dim_{\phi m} \mathcal{H} &\leq \dim_{\phi} \mathcal{E}^{\circ} \leq \dim_{\phi} \mathcal{E}, \\ \dim_{\phi m} \mathcal{H} - \dim_{1m} \mathcal{H} &\leq \dim_1 \mathcal{E}^{\circ} \leq \dim_1 \mathcal{E}. \end{aligned}$$

Pour calculer $\dim_1 \mathcal{E}$ et $\dim_{\phi} \mathcal{E}$, on peut appliquer le théorème II. Mais dans ce cas particulier, il suffit d'utiliser la proposition IIb. On a un isomorphisme : $\mathcal{E}^1 \cong \mathcal{E}_{L_o}$ et $\mathcal{E}$ est produit direct : $\mathcal{E} = \mathcal{E}^1 \mathcal{E}^{\phi}$. Nous

aurons donc: $\dim_1 \mathcal{E} = \dim_{\ell} \mathcal{E}^1 = \dim_{\ell} \mathcal{E}_{L_0} = \dim_{\mathbb{Z}} E_{L_0}$, puisque L_0 ne peut contenir de racine $\ell^{\text{ème}}$ de 1. D'autre part, puisque L contient une racine $\ell^{\text{ème}}$ de 1 : $\dim_{\ell} \mathcal{E} = \dim_{\mathbb{Z}} E_L + 1$. D'où:

$$\dim_{\phi} \mathcal{E} = \dim_{\ell} \mathcal{E} - \dim_{\ell} \mathcal{E}^1 = \dim_{\mathbb{Z}} E_L - \dim_{\mathbb{Z}} E_{L_0} + 1.$$

Supposons maintenant que $\mathcal{S}$ ne soit pas une unité ℓ -primaire de L , c'est-à-dire que $L(\sqrt[\ell]{\mathcal{S}})/L$ soit ramifiée. Considérons le $\mathbb{F}_{\ell}[G]$ -module $\mathcal{E}/\mathcal{E}^{\circ}$, isomorphe à E/E° . Le sous-module de E/E° engendré par la classe de $\mathcal{S}$ modulo E° n'est pas réduit à 1 et a pour caractère: $\chi^* = \phi$. Il s'en suit que $\mathcal{E}/\mathcal{E}^{\circ}$ contient un $\mathbb{F}_{\ell}[G]$ -module simple de caractère $\chi^* = \phi$. Comme le caractère de $\mathcal{E}$ est $\psi_L = \chi^* + \psi_0 - 1$, le caractère de $\mathcal{E}^{\circ}$ est "au plus" $\psi_0 - 1$ et on a: $\dim_{\phi} \mathcal{E}^{\circ} \leq \dim_{\phi} \mathcal{E} - 1$.

Remarques. La dernière hypothèse: " $\mathcal{S}$ n'est pas une unité ℓ -primaire de L " est vérifiée en particulier dans le cas où L est le ℓ^n ème corps cyclotomique. Par exemple, pour $n = 1$, nous obtenons:

Si $\mathcal{H}_0$ et $\mathcal{H}^*$ sont les ℓ -groupes des classes réelles et relatives de $\mathbb{Q}^{(\ell)}$, la différence des ℓ -rangs de ces groupes est bornée par:

$$0 \leq \dim_{\ell} \mathcal{H}^* - \dim_{\ell} \mathcal{H}_0 \leq (\ell - 3)/2.$$

Ces inégalités ont été obtenues par Hecke; [5].

Kummer avait déjà montré que si ℓ divise le nombre de classes réelles de $\mathbb{Q}^{(\ell)}$, alors ℓ divise également le nombre de classes relatives de $\mathbb{Q}^{(\ell)}$. Ce résultat lui permettait de caractériser les nombres premiers ℓ divisant le nombre de classes de $\mathbb{Q}^{(\ell)}$ (nombres premiers irréguliers) au moyen des nombres de Bernoulli. Il l'obtenait à l'aide des formules analytiques; ([1] Ch 5 § 6).

Signalons encore l'existence d'une autre "propriété de Kummer": ℓ étant toujours un nombre premier impair et n un entier quelconque, si le nombre de classes réelles du ℓ^n ème corps cyclotomique est pair, alors le nombre de classes relatives de ce même corps est également pair. Ceci peut se démontrer facilement à l'aide de la formule des classes ambiges appliquée à l'extension: $\mathbb{Q}^{(\ell^n)} / \mathbb{Q}_0^{(\ell^n)}$. Toutefois, pour étudier ce type de question, les méthodes utilisant les formules analytiques paraissent plus précises. On peut voir par exemple: [4] § 37 et 38.

3. Comparaison des 3-groupes des classes de $k(\sqrt{d})$ et $k(\sqrt{-3d})$.

Proposition V c. Soit k un corps de nombres ne contenant pas $\sqrt{-3}$.

Soit d un élément de k tel que ni $\sqrt{d}$, ni $\sqrt{-3d}$ n'appartiennent à k .

Posons $K = k(\sqrt{d})$, $\bar{K} = k(\sqrt{-3d})$ et $k' = k(\sqrt{-3})$. Soient $\mathcal{H}_K$, $\mathcal{H}_{\bar{K}}$, $\mathcal{H}_{k'}$, $\mathcal{H}_k$ les 3-groupes des classes d'idéaux de K , $\bar{K}$, k' et k .

Soient j , $\bar{j}$, j' les injections canoniques de $\mathcal{H}_k$ dans $\mathcal{H}_K$, $\mathcal{H}_{\bar{K}}$, $\mathcal{H}_{k'}$.

Pour toute puissance de 3, notée m et telle que le sous-corps réel maximal du $m^{\text{ème}}$ corps cyclotomique soit contenu dans k , on a les inégalités :

$$(1) \dim_m \mathcal{H}_{\bar{K}} / \bar{j}(\mathcal{H}_k) - \dim_m \mathcal{H}_K / j(\mathcal{H}_k) \leq \dim_{\mathbb{Z}} E_K - \dim_{\mathbb{Z}} E_k,$$

$$(2) \dim_m \mathcal{H}_k - \dim_m \mathcal{H}_{k'} / j'(\mathcal{H}_k) \leq \dim_{\mathbb{Z}} E_{k'} - \dim_{\mathbb{Z}} E_k + 1,$$

$$(3) \dim_m \mathcal{H}_{k'} / j'(\mathcal{H}_k) - \dim_m \mathcal{H}_k \leq \dim_{\mathbb{Z}} E_k.$$

Les quantités $\dim_{\mathbb{Z}} E_K$, $\dim_{\mathbb{Z}} E_{k'}$, $\dim_{\mathbb{Z}} E_k$ sont les dimensions des $\mathbb{Z}$ -modules libres, quotients des groupes des unités : E_K , $E_{k'}$, E_k de K , k' et k par leurs sous-groupes de torsion.

Démonstration. Posons $L = k(\sqrt{d}, \sqrt{-3d})$ et $G = \text{Gal}(L/k)$. Ce groupe est un groupe de Klein. Notons ses éléments de la façon suivante : $G = \{1, \sigma, \bar{\sigma}, \sigma\bar{\sigma}\}$ et supposons que σ invarie K et $\bar{\sigma}$ invarie $\bar{K}$. Soient $1, \phi, \bar{\phi}, \chi^*$ les caractères irréductibles de G sur $\mathbb{Q}_3$ définis par le tableau suivant :

	1	σ	$\bar{\sigma}$	$\sigma\bar{\sigma}$
1	1	1	1	1
χ^*	1	-1	-1	1
ϕ	1	1	-1	-1
$\bar{\phi}$	1	-1	1	-1

Soit n le plus grand entier tel que le sous-corps réel maximal $\mathbb{Q}_o^{(3^n)}$ du $3^n^{\text{ème}}$ corps cyclotomique soit inclus dans k . Soit ζ une racine primitive $3^n^{\text{ème}}$ de 1. Elle appartient à L . Le caractère miroir de L/k est χ^* et $1, \chi^*$ d'une part, ϕ et $\bar{\phi}$ d'autre part, sont reflets l'un

de l'autre . Appliquons le théorème III à L/k , avec $\ell = 3$. On obtient les inégalités : ($\mathcal{H}$ et $\mathcal{E}$ désignent le groupe des ℓ -classes et le groupe des ℓ -unités de L)

$$\begin{aligned} \dim_{\bar{\phi}_m} \mathcal{H} - \dim_{\phi_m} \mathcal{H} &\leq \dim_{\phi} \mathcal{E} , \\ \dim_{1m} \mathcal{H} - \dim_{\chi^*_m} \mathcal{H} &\leq \dim_{\chi^*} \mathcal{E} , \\ \dim_{\chi^*_m} \mathcal{H} - \dim_{1m} \mathcal{H} &\leq \dim_1 \mathcal{E} , \end{aligned}$$

pour toute puissance de 3 notée m et inférieure à 3^n .

D'après la proposition II a nous avons $\mathcal{H}_K = \mathcal{H}^1 \mathcal{H}^{\phi}$, (en considérant $\mathcal{H}_K$ comme un sous-groupe de $\mathcal{H}$) et $\mathcal{H}^1 = j(\mathcal{H}_k)$ d'où : $\mathcal{H}^{\phi} \cong \mathcal{H}_K / j(\mathcal{H}_k)$ et $\dim_{\phi_m} \mathcal{H} = \dim_m \mathcal{H}_K / j(\mathcal{H}_k)$. On interprète de la même façon les quantités : $\dim_{\bar{\phi}_m} \mathcal{H}$, $\dim_{1m} \mathcal{H}$, $\dim_{\chi^*_m} \mathcal{H}$.

Soit i l'injection canonique de $\mathcal{E}_k$ dans $\mathcal{E}_K$. Considérons $\mathcal{E}_K$ comme un sous-groupe de $\mathcal{E}$, nous aurons $\mathcal{E}_K = \mathcal{E}^{\phi} \mathcal{E}^1$ et $\mathcal{E}^1 = i(\mathcal{E}_k)$ (proposition II b) . Nous en déduisons $\mathcal{E}^{\phi} \cong \mathcal{E}_K / i(\mathcal{E}_k)$ et $\dim_{\phi} \mathcal{E} = \dim_3 \mathcal{E}^{\phi} = \dim_3 \mathcal{E}_K - \dim_3 \mathcal{E}_k$. Remarquons enfin que ni K , ni k ne contiennent de racine cubique de 1 . Il s'en suit que : $\dim_3 \mathcal{E}_K = \dim_{\mathbb{Z}} E_K$ et $\dim_3 \mathcal{E}_k = \dim_{\mathbb{Z}} E_k$. On a donc : $\dim_{\phi} \mathcal{E} = \dim_{\mathbb{Z}} E_K - \dim_{\mathbb{Z}} E_k$.

La quantité $\dim_{\chi^*} \mathcal{E}$ s'interprète de la même façon . La seule différence est que k' contient les racines cubiques de 1 et : $\dim_3 \mathcal{E}_{k'} = \dim_{\mathbb{Z}} E_{k'} + 1$.

Remarques . De même qu'à la proposition précédente , on peut ajouter que si $\mathcal{S}$ n'est pas une unité 3-primaire de k' , alors le chiffre 1 apparaissant dans l'égalité (2) peut être remplacé par 0 .

Dans le cas particulier où $k = \mathbb{Q}$, les inégalités (2) et (3) deviennent triviales . Il reste , si $K = \mathbb{Q}(\sqrt{d})$ et $\bar{K} = \mathbb{Q}(\sqrt{-3d})$, avec d rationnel positif , les inégalités :

$$0 \leq \dim_3 \mathcal{H}_{\bar{K}} - \dim_3 \mathcal{H}_K \leq 1 .$$

Ce résultat est du à Scholtz ([8]) .

Bibliographie.

- [1] Borevitch (Z.I.) et Chafarevitch (I.R.) , Théorie des nombres , Gauthier-Villars , Paris , (1967).
- [2] Bouvier (L.) , Généralisation d'une inégalité de Hecke sur les nombres de classes , Séminaire de Théorie des Nombres de Grenoble . (1969) .
- [3] Curtis (C.W.) and Reiner (I.) , Representation theory of finite groups and associative algebras , Interscience Publishers, (1962).
- [4] Hasse (H.) , Über die Klassenzahl abelscher Zahlkörpern , Berlin , (1952) .
- [5] Hecke (E.) , Über nicht-reguläre Primzahlen und den Fermatschen Satz , Gött. Nachr. Math. Phys. Kl. (1910) 420-424 .
- [6] Leopoldt (H.W.) Zur Struktur der ℓ -Klassengruppe galoisscher Zahlkörper , Journ. für die reine und ang. Math. 199 , (1958).
- [7] Oriat (B.) , Quelques caractères utiles à l'arithmétique , Publications Mathématiques de la Faculté de Besançon , (1974).
- [8] Scholtz (A.) Über die Beziehung der Klassenzahlen quadratischer Körper zueinander , Journ. für die reine und ang. Math. 166 , (1931) 201-203 .
- [9] Serre (J.P.) , Représentations linéaires des groupes finis , Hermann , (1971) .

RELATION ENTRE LES 2-GROUPES DES CLASSES D'IDÉAUX AU SENS ORDINAIRE ET RESTREINT DE CERTAINS CORPS DE NOMBRES

PAR
BERNARD ORIAT
[Besançon]

RÉSUMÉ. — Les résultats obtenus par J. V. ARMITAGE et A. FRÖHLICH dans un article intitulé *Class Numbers and Unit signatures* sont démontrés d'une autre façon et généralisés. La méthode utilisée ici est issue du *Spiegelungssatz* de H. W. LEOPOLDT.

Soit $K/\mathbb{Q}$ une extension galoisienne, de groupe de Galois G contenant les racines l -ième de l'unité (l premier), et telle que son degré soit premier à l . C'est sous ces hypothèses que LEOPOLDT a énoncé et démontré le *Spiegelungssatz* [4]. Cette propriété repose essentiellement sur l'utilisation de la structure de module sur l'algèbre semi-simple $\mathbb{F}_l[G]$. Le groupe $\mathfrak{H}_l$ des classes h de K telles que $h^l = 1$ est un tel module. Si E est le groupe des unités de K et E_0 le sous-groupe des unités l -primaires de K , E_0/E^l est aussi un tel module. Soit Φ un caractère irréductible de G sur $\mathbb{F}_l$, et si H est un $\mathbb{F}_l[G]$ -module soit $\dim_{\Phi}(H)$ le nombre de sous-modules simples de caractère Φ intervenant dans une décomposition de H en somme directe de modules simples. LEOPOLDT a défini une involution : $\Phi \rightarrow \bar{\Phi}$ de l'ensemble des caractères irréductibles de G sur $\mathbb{F}_l$, et a obtenu la majoration suivante :

$$\dim_{\bar{\Phi}}(\mathfrak{H}_l) - \dim_{\Phi}(\mathfrak{H}_l) \leq \dim_{\Phi}(E_0/E^l).$$

Le cas $l = 2$ n'est pas exclu par LEOPOLDT. Toutefois celui-ci n'a considéré que des classes d'idéaux au sens ordinaire. Il nous a semblé nécessaire d'introduire, dans ce cas, les deux groupes : $\mathfrak{H}_2$ (resp. $\mathfrak{H}'_2$) des classes d'idéaux de K au sens restreint (resp. au sens ordinaire) dont le carré est la classe principale au sens restreint (resp. au sens ordinaire). Nous obtenons alors (G étant supposé d'ordre impair), l'inégalité suivante :

$$\dim_{\Phi}(\mathfrak{H}_2) - \dim_{\Phi}(\mathfrak{H}'_2) + \dim_{\bar{\Phi}}(\mathfrak{H}_2) - \dim_{\bar{\Phi}}(\mathfrak{H}'_2) \leq \chi(1),$$

où $\chi(1)$ désigne le degré du caractère absolument irréductible dont Φ est issu.

Cette inégalité permet de retrouver et généraliser les résultats d'ARMITAGE et FRÖHLICH [1]. Ceux-ci supposaient G cyclique d'ordre une puissance d'un nombre premier impair.

Dans le cas où G est abélien d'ordre impair, M. TAYLOR a généralisé dans [6] la démonstration de J.-P. SERRE (celle-ci se trouve dans [1]). Il a obtenu les résultats que nous avons noté corollaires 2 a et 2 b.

Georges GRAS m'a guidé vers le *Spiegelungssatz*. Ses conseils m'ont été précieux. Je l'en remercie vivement.

1. Préliminaires

1.1. *Notations.* — On désigne par K un corps de nombres. Le 2-groupe des classes au sens ordinaire (resp. au sens restreint) de K est noté $\mathfrak{H}'$ (resp. $\mathfrak{H}$). De même, l'ensemble des éléments h de $\mathfrak{H}'$ (resp. $\mathfrak{H}$) tel que $h^2 = 1$ est noté $\mathfrak{H}'_2$ (resp. $\mathfrak{H}_2$). On désigne par P' (resp. P) l'ensemble des idéaux principaux (resp. strictement principaux) de K .

L'extension abélienne d'exposant 2 maximale de K , dans laquelle aucune place (resp. aucun idéal) ne se ramifie, est notée M' (resp. M). Ces extensions sont des extensions de Kummer, et on désigne par W' et W leurs radicaux, c'est-à-dire

$$W' = \{ \omega; \omega \in M', \omega^2 \in K \} \quad \text{et} \quad W = \{ \omega; \omega \in M, \omega^2 \in K \}.$$

Le nombre de places réelles de K est noté r , et l'application $S: K \rightarrow \{ \pm 1 \}^r$ est la signature de K . Le groupe des unités (resp. des unités totalement positives, des unités 2-primaires) de K est noté E (resp. E^+ , E_0). On désigne par γ l'application canonique de $\mathfrak{H}$ dans $\mathfrak{H}'$ qui associe à la classe au sens restreint de l'idéal α de K , la classe ordinaire de α . Enfin $\dim_2 H$ désignera la dimension sur $\mathbb{F}_2$ du $\mathbb{F}_2$ -espace vectoriel H .

1.2. *Rappels.* — En associant à l'idéal de K engendré par x , la classe modulo $S(E)$ de $S(x)$, on définit un isomorphisme

$$(1 a) \quad P'/P \cong S(K)/S(E).$$

D'autre part, P'/P est inclus dans $\mathfrak{H}_2$, et on a donc

$$(1 b) \quad \gamma(\mathfrak{H}_2) \cong \mathfrak{H}_2/(P'/P).$$

Enfin, en appliquant la théorie de Kummer et la théorie du corps de classe, on obtient les isomorphismes

$$(1 c) \quad W/K \cong \text{Gal}(M/K) \cong \mathfrak{H}/\mathfrak{H}^2; \quad W'/K \cong \text{Gal}(M'/K) \cong \mathfrak{H}'/\mathfrak{H}'^2.$$

(On désigne encore par K le groupe multiplicatif de K .)

1.3. *Définition des applications θ et ψ .* — Si ω appartient à W , l'extension $K(\omega)/K$ est non ramifiée pour les idéaux. L'idéal de K engendré par ω^2 est donc le carré d'un idéal α de K . En associant à ω K la classe (ordinaire) de α , on définit un homomorphisme de W/K dans $\mathfrak{H}'_2$. De plus, si ω appartient à W' , ω^2 est totalement positif, et la classe de l'idéal α appartient à $\gamma(\mathfrak{H}_2)$. Nous avons donc défini un homomorphisme θ :

$$\theta : (W/K)/(W'/K) \rightarrow \mathfrak{H}'_2/\gamma(\mathfrak{H}_2),$$

qui associe à ω $K(W'/K)$ la classe, modulo $\gamma(\mathfrak{H}_2)$, de la classe de α .

Si maintenant ω $K(W'/K)$ appartient au noyau de θ , il existera un élément totalement positif a de K et une unité ε de K tels que : $\omega^2 = a\varepsilon$. En associant εE^+ à ω $K(W'/K)$, on définit un homomorphisme injectif ψ :

$$\psi : \text{Ker } \theta \rightarrow E/E^+.$$

2. Cas général

On suppose dans ce paragraphe que K est un corps de nombres quelconque. On déduit des isomorphismes (1 a), (1 b), (1 c) les égalités

$$(2a) \quad \dim_2(P'/P) = r - \dim_2(E/E^+),$$

$$(2b) \quad \dim_2(\gamma(\mathfrak{H}_2)) = \dim_2(\mathfrak{H}_2) - \dim_2(P'/P),$$

$$(2c) \quad \dim_2((W/K)/(W'/K)) = \dim_2(\mathfrak{H}_2) - \dim_2(\mathfrak{H}'_2).$$

D'autre part, en utilisant les applications θ et ψ , on obtient :

$$\dim_2((W/K)/(W'/K)) - \dim_2(E/E^+) \leq \dim_2(\mathfrak{H}'_2) - \dim_2(\gamma(\mathfrak{H}_2)).$$

En utilisant cette inégalité et les égalités (2 a), (2 b), (2 c), on obtient le théorème suivant :

THÉORÈME 1. — Les 2-rangs des groupes $\mathfrak{H}$ et $\mathfrak{H}'$ sont reliés par

$$\dim_2(\mathfrak{H}_2) - \dim_2(\mathfrak{H}'_2) \leq r/2.$$

COROLLAIRE 1 a. — Les 2-rangs des groupes $\mathfrak{H}'$ et E/E^+ sont reliés par

$$\dim_2(\mathfrak{H}'_2) \geq r/2 - \dim_2(E/E^+).$$

COROLLAIRE 1 b. — Les 2-rangs des groupes $\mathfrak{H}'$ et E_0/E^2 sont reliés par

$$\dim_2(\mathfrak{H}'_2) \geq \dim_2(E_0/E^2) - (r/2).$$

Ces corollaires se déduisent du théorème 1. Le premier est obtenu en utilisant (2 a) et (2 b) et en minorant $\gamma(\mathfrak{H}_2)$ par 0. Pour démontrer le deuxième, on utilise l'injection de E_0/E^2 dans W/K qui associe $\sqrt{\varepsilon} K$ à εE^2 .

On retrouve ainsi les résultats I, II, III de [1].

3. Cas galoisien

On suppose donc maintenant $K/\mathbb{Q}$ galoisienne de degré impair.

3.1. *Rappels et notations.* — On désignera par G le groupe de Galois de $K/\mathbb{Q}$. Ce groupe est donc d'ordre impair, et l'algèbre $\mathbb{F}_2[G]$ est semi-simple. Soit Φ un caractère irréductible de G sur $\mathbb{F}_2$. Il est le résidu modulo 2 d'un caractère irréductible Φ' de G sur le corps des nombres 2-adiques $\mathbb{Q}_2$. On désignera par χ un caractère de G absolument irréductible au-dessus de Φ' . Si $\mathbb{Q}_2(\chi)$ est le corps des valeurs de χ (c'est-à-dire

$$\mathbb{Q}_2(\chi) = \mathbb{Q}_2(\chi(\sigma))_{\sigma \in G},$$

on rappelle que $\mathbb{Q}_2(\chi)$ est l'extension non ramifiée de $\mathbb{Q}_2$ de degré $\Phi'(1)/\chi(1)$, et que Φ' est la trace relative à $\mathbb{Q}_2(\chi)/\mathbb{Q}_2$ de χ .

Posons $1_\Phi = \sum_{\sigma \in G} \Phi(\sigma^{-1}) \sigma$. Cet élément de $\mathbb{F}_2[G]$ est l'idempotent central primitif associé à Φ . Il est le résidu modulo 2 de l'idempotent

$$1_{\Phi'} = (\chi(1)/|G|) \sum_{\sigma \in G} \Phi'(\sigma^{-1}) \sigma \quad \text{de l'algèbre } \mathbb{Q}_2[G].$$

Si H est un $\mathbb{F}_2[G]$ module, on désignera par H^Φ la composante de H relative à Φ , c'est-à-dire $H^\Phi = H 1_\Phi$ (ou $H^\Phi = H^{1_\Phi}$ si H est noté multiplicativement). Ce module H est alors somme directe des H^Φ , Φ parcourant l'ensemble des caractères irréductibles de G sur $\mathbb{F}_2$. On désignera par $\dim_\Phi(H)$ le nombre de $\mathbb{F}_2[G]$ -modules simples dont H^Φ est somme directe. On a la relation

$$\dim_2(H^\Phi) = \Phi'(1) \dim_\Phi(H).$$

Considérons par exemple E/E^2 . Comme les seules racines de 1 contenues dans K sont ± 1 , on déduit du théorème de Dirichlet que G opère « régulièrement » sur E/E^2 (c'est-à-dire que le caractère de E/E^2 est le caractère de la représentation régulière de G). On a donc

$$\dim_\Phi(E/E^2) = \chi(1).$$

De plus, E/E^+ est un $\mathbb{F}_2[G]$ -module et c'est un quotient de E/E^2 . On a donc

$$\dim_\Phi(E/E^+) \leq \chi(1).$$

Si on munit $S(K)$ de la structure de $\mathbb{F}_2[G]$ -module obtenue en posant $S(x)^\sigma = S(x^\sigma)$ pour tout σ de G , alors G opérera aussi « régulièrement » sur $S(K)$. Les deux isomorphismes (1 a) et (1 b) sont maintenant des $\mathbb{F}_2[G]$ isomorphismes, et on a

$$(3 a) \quad \dim_\Phi(P'/P) = \chi(1) - \dim_\Phi(E/E^+),$$

$$(3 b) \quad \dim_\Phi(\gamma(\mathfrak{H}_2)) = \dim_\Phi(\mathfrak{H}_2) - \dim_\Phi(P'/P).$$

L'extension M/Q est galoisienne, et tout σ appartenant à G admet un prolongement s à M . En posant $(\omega K)^\sigma = \omega^s K$, on définit une structure de $F_2[G]$ -module sur W/K . Dans [4], LEOPOLDT a défini le *Spiegelbild* $\bar{\Phi}$ de Φ . Comme nous sommes dans le cas $l = 2$, on a donc

$$\bar{\Phi}(\sigma) = \Phi(\sigma^{-1}) \quad \text{pour tout } \sigma \text{ de } G.$$

On peut introduire de même $\bar{\Phi}'$ et $\bar{\chi}$. On rappelle que $\bar{\Phi}$ est encore un caractère irréductible de G sur F_2 , que $\bar{\Phi} = \Phi$ et que $\chi(1) = \bar{\chi}(1)$.

L'isomorphisme (1 c) : $W/K \cong \mathfrak{H}/\mathfrak{H}^2$ n'est pas un $F_2[G]$ -isomorphisme, mais il envoie $(W/K)^\Phi$ sur $(\mathfrak{H}/\mathfrak{H}^2)^{\bar{\Phi}}$. LEOPOLDT a appelé cette propriété : *Spiegelungsrelation*, et en a donné la démonstration dans [4]. Ceci est encore vrai pour W'/K et $\mathfrak{H}'/\mathfrak{H}'^2$.

On en déduit l'égalité

$$(3c) \quad \dim_\Phi((W/K)/(W'/K)) = \dim_{\bar{\Phi}}(\mathfrak{H}_2) - \dim_{\bar{\Phi}}(\mathfrak{H}'_2).$$

3.2. *Utilisation des applications θ et ψ .* — Ces applications sont définies en 1.3. Ce sont désormais des $F_2[G]$ -homomorphismes. On obtient alors l'inégalité :

$$\dim_\Phi((W/K)/(W'/K)) - \dim_\Phi(E/E^+) \leq \dim_\Phi(\mathfrak{H}'_2) - \dim_\Phi(\gamma(\mathfrak{H}_2)).$$

En utilisant (3 a), (3 b), (3 c), on en déduit le théorème suivant.

THÉORÈME 2. — *Les nombres de $F_2[G]$ -modules simples de caractère Φ ou $\bar{\Phi}$ intervenant dans une décomposition de $\mathfrak{H}_2$ et $\mathfrak{H}'_2$ en somme directe de modules simples sont liés par la relation*

$$\dim_\Phi(\mathfrak{H}_2) - \dim_\Phi(\mathfrak{H}'_2) + \dim_{\bar{\Phi}}(\mathfrak{H}_2) - \dim_{\bar{\Phi}}(\mathfrak{H}'_2) \leq \chi(1).$$

On en déduit, en utilisant (3 a) (3 b) et en minorant $\dim_\Phi(\gamma(\mathfrak{H}_2))$ par O , le résultat suivant.

COROLLAIRE 2 a :

$$\dim_\Phi(\mathfrak{H}'_2) + \dim_{\bar{\Phi}}(\mathfrak{H}'_2) \geq \chi(1) - \dim_\Phi(E/E^+) - \dim_{\bar{\Phi}}(E/E^+).$$

D'autre part, l'injection de E_0/E^2 dans W/K , qui associe $\sqrt{\varepsilon} K$ à εE^2 est un $F_2[G]$ -homomorphisme. On a donc

$$\dim_\Phi(E_0/E^2) \leq \dim_\Phi(W/K) = \dim_{\bar{\Phi}}(\mathfrak{H}_2).$$

On déduit du théorème 2 le corollaire suivant :

COROLLAIRE 2 b :

$$\dim_\Phi(\mathfrak{H}'_2) + \dim_{\bar{\Phi}}(\mathfrak{H}'_2) \geq \dim_\Phi(E_0/E^2) + \dim_{\bar{\Phi}}(E_0/E^2) - \chi(1).$$

Remarque. — Comme $\dim_{\Phi}(E/E^2) = \chi(1)$, on a
 $\chi(1) - \dim_{\Phi}(E/E^+) - \dim_{\bar{\Phi}}(E/E^+) = \dim_{\Phi}(E^+/E^2) + \dim_{\bar{\Phi}}(E^+/E^2) - \chi(1)$.

On a une relation analogue, obtenue en remplaçant E^+ par E_0 .

3.3. Cas particuliers.

(i) *Supposons G abélien.* Les caractères irréductibles de G sont alors de degré 1. On a donc $\chi(1) = 1$. Le théorème 2 peut alors s'énoncer :

L'une au moins des différences

$$\dim_{\Phi}(\mathfrak{H}_2) - \dim_{\Phi}(\mathfrak{H}'_2) \quad \text{ou} \quad \dim_{\bar{\Phi}}(\mathfrak{H}_2) - \dim_{\bar{\Phi}}(\mathfrak{H}'_2)$$

est égale à 0. L'autre ne peut valoir que 0 ou 1.

De même, le corollaire 2 a peut s'énoncer :

L'une au moins des inégalités

$$\dim_{\Phi}(\mathfrak{H}'_2) \geq \dim_{\Phi}(E^+/E^2) \quad \text{ou} \quad \dim_{\bar{\Phi}}(\mathfrak{H}'_2) \geq \dim_{\bar{\Phi}}(E^+/E^2)$$

est vraie.

Il en est de même pour le corollaire 2 b.

Ces corollaires ont été obtenus par M. TAYLOR [6]. On retrouve également ainsi la condition suffisante de parité de [3] (corollaire IV.3).

Les caractères absolument irréductibles de G forment un groupe. Soit g_{χ} l'ordre de χ . Le corps des valeurs de χ est le corps cyclotomique $\mathbf{Q}_2^{(g_{\chi})}$ obtenu en ajoutant à $\mathbf{Q}_2$ les racines g_{χ} -ième de 1. Le groupe de Galois de $\mathbf{Q}_2^{(g_{\chi})}/\mathbf{Q}_2$ est isomorphe au sous-groupe de $(\mathbf{Z}/g_{\chi}\mathbf{Z})^*$ engendré par la classe de 2 modulo g_{χ} . Ce sous-groupe contient la classe de -1 modulo g_{χ} si, et seulement si, χ est conjugué de $\bar{\chi} = \chi^{-1}$. Autrement dit, Φ est égal à $\bar{\Phi}$ si, et seulement si, il existe une puissance de 2 congrue à -1 modulo g_{χ} .

Si cette condition est vérifiée, on aura alors :

$$\begin{aligned} \dim_{\Phi}(\mathfrak{H}_2) &= \dim_{\Phi}(\mathfrak{H}'_2), \\ \dim_{\Phi}(\mathfrak{H}'_2) &\geq \dim_{\Phi}(E^+/E^2), \\ \dim_{\Phi}(\mathfrak{H}'_2) &\geq \dim_{\Phi}(E_0/E^2). \end{aligned}$$

COROLLAIRE 2 c. — *Supposons G d'exposant e . On a alors : -1 est congru à une puissance de 2 modulo e si, et seulement si, $\Phi = \bar{\Phi}$ pour tout caractère Φ irréductible de G sur $\mathbf{F}_2$. Si cette condition est vérifiée, on aura*

$$\begin{aligned} \dim_2(\mathfrak{H}_2) &= \dim_2(\mathfrak{H}'_2), \\ \dim_2(\mathfrak{H}'_2) &\geq \dim_2(E^+/E^2), \\ \dim_2(\mathfrak{H}'_2) &\geq \dim_2(E_0/E^2). \end{aligned}$$

Ces dernières relations s'obtiennent en effectuant la somme des précédentes sur les différents caractères Φ de G . On retrouve ainsi les résultats IV et V de [1].

(ii) Supposons G non commutatif d'ordre pq (p et q étant premiers et impairs). Dans ce cas, nous avons vérifié que $\Phi = \bar{\Phi}$ pour tout caractère Φ irréductible de G sur F_2 si, et seulement si, les ordres de 2 modulo p et q sont pairs. Si cette condition est vérifiée, nous obtenons les inégalités :

$$\begin{aligned} \dim_2(\mathfrak{H}_2) - \dim_2(\mathfrak{H}'_2) &\leq (p-1)(q-1)/2, \\ \dim_2(\mathfrak{H}'_2) &\geq \dim_2(E^+/E^2) - (p-1)(q-1)/2, \\ \dim_2(\mathfrak{H}'_2) &\geq \dim_2(E_0/E^2) - (p-1)(q-1)/2. \end{aligned}$$

BIBLIOGRAPHIE

- [1] ARMITAGE (J.-V.) and FRÖHLICH (A.). — Class numbers and unit signatures *Mathematika*, London, t. 14, 1967, p. 94-98.
- [2] GRAS (G. et M.-N.). — Signature des unités cyclotomiques et parité du nombre de classes des extensions cycliques de $\mathbb{Q}$ de degré premier impair, *Annales Inst. Fourier*, Grenoble, t. 25, 1975, fasc. 1.
- [3] GRAS (G.). — Critère de parité du nombre de classes des extensions abéliennes de $\mathbb{Q}$ de degré impair, *Bull. Soc. math. France*, t. 103, 1975, p. 177-190.
- [4] LEOPOLDT (H.-W.). — Zur Struktur der l -Klassengruppe Galoischer Zahlkörper, *J. für die reine und angew. Math.*, t. 199, 1958, p. 165-174.
- [5] SERRE (J.-P.). — *Représentations linéaires des groupes finis*. — Paris, Hermann, 1967 (Collection « Méthodes », Mathématiques).
- [6] TAYLOR (M.). — *Galois module structure of class groups and units* (à paraître).

(Texte reçu le 19 septembre 1975).

Bernard ORIAT,
Faculté des Sciences,
Mathématiques,
Route de Gray,
25030 Besançon.

RELATIONS ENTRE LES 2-GROUPES DES CLASSES D'IDÉAUX DES EXTENSIONS QUADRATIQUES

$k(\sqrt{d})$ ET $k(\sqrt{-d})$

par Bernard ORIAT

D'une façon générale nous désignerons par $\mathcal{H}_L$ le 2-groupe des classes au sens restreint du corps de nombres L . Soit a un entier sans facteur carré positif. P. Damey et J. J. Payan ont montré dans [2] que la différence des 4-rangs : $\dim_4 \mathcal{H}_{\mathbb{Q}(\sqrt{-a})} - \dim_4 \mathcal{H}_{\mathbb{Q}(\sqrt{a})}$ ne peut prendre que l'une ou l'autre des valeurs 1 ou 0. L. Bouvier a montré dans [1] que pour $m = 4$ et 8 les différences des m -rangs : $\dim_m \mathcal{H}_{\mathbb{Q}(\sqrt{a}, \sqrt{-a})} - \dim_m \mathcal{H}_{\mathbb{Q}(\sqrt{a}, \sqrt{a})}$ sont comprises entre 0 et 4.

Nous généralisons ci-après ces propriétés. Pour énoncer le résultat obtenu, fixons quelques notations. On désignera par :

k un corps de nombres ne contenant pas $\sqrt{-1}$,

d un élément de k tel que ni $\sqrt{d}$, ni $\sqrt{-d}$ n'appartiennent à k ,

$K = k(\sqrt{d})$, $\bar{K} = k(\sqrt{-d})$,

j (resp $\bar{j}$) l'application de $\mathcal{H}_k$ dans $\mathcal{H}_K$ (resp. $\mathcal{H}_{\bar{K}}$) déduite de l'injection canonique du groupe des idéaux de k dans le groupe des idéaux de K (resp. $\bar{K}$).

Posons $\mathcal{D} = \mathcal{H}_K / j(\mathcal{H}_k)$ et $\bar{\mathcal{D}} = \mathcal{H}_{\bar{K}} / \bar{j}(\mathcal{H}_k)$.

Nous démontrons que pour toute puissance de 2, notée m , supérieure ou égale à 4, et telle que le sous-corps réel maximal du $m^{\text{ème}}$ corps cyclotomique $\mathbb{Q}_0^{(m)}$ soit inclus dans k , la différence des m -rangs de $\mathcal{D}$ et $\bar{\mathcal{D}}$ est majorée par la

somme de trois constantes positives ou nulles :

$$\dim_m \mathcal{D} - \dim_m \overline{\mathcal{D}} \leq n_1 + n_2 + n_3.$$

Si $E_{\overline{k}}$ et E_k sont les groupes d'unités de $\overline{k}$ et k , n_1 a pour valeur $n_1 = \dim_{\mathbf{Z}}(E_{\overline{k}}) - \dim_{\mathbf{Z}}(E_k)$. On trouvera les définitions de n_2 et n_3 au début du paragraphe 3. Précisons simplement pour l'instant que lorsque k est 2-principal, c'est-à-dire lorsque $\mathcal{H}_k = 1$, alors n_3 est nul et $\mathcal{D}$ (resp. $\overline{\mathcal{D}}$) coïncide avec $\mathcal{H}_k$ (resp. $\mathcal{H}_{\overline{k}}$). Si de plus k est totalement réel, alors n_2 est nul également. C'est ce qui se passe lorsque $k = \mathbf{Q}$ ou $\mathbf{Q}(\sqrt{2})$ et on retrouve alors les résultats cités ci-dessus.

Pour démontrer leur propriété, Damey et Payan ont utilisé une construction et un dénombrement des extensions non ramifiées cycliques de degré 4 d'un corps quadratique.

D'autre part, G. Gras a donné, de cette même propriété, une démonstration employant la loi de réciprocité quadratique; [3]. L. Bouvier avait utilisé des techniques analogues à celles de Damey-Payan.

La méthode que nous employons diffère de celles-ci. Elle emprunte pour l'essentiel au « Spiegelungssatz » de Leopoldt [4]. Toutefois, celui-ci pose une hypothèse : « l ne divise pas $|G|$ » qui assure la semi-simplicité des $\mathbf{F}_l[G]$ -modules considérés et qui n'est pas vérifiée ici.

Le groupe $\mathcal{D}/\mathcal{D}^m$ est considéré à l'aide de l'isomorphisme de réciprocité, comme le groupe de Galois d'une extension non ramifiée de K notée N_m . Si l'on pose $L = K(\sqrt{-1})$, $G = \text{Gal}(L/k)$ et $M_m = N_m(\sqrt{-1})$, alors M_m/L est une extension de Kummer et on désigne par W_m son radical. Le m -rang de $\mathcal{D}$ est alors représenté par le 2-rang de $W_m/W_{m/2}$. L'application θ_m dérive d'une application déjà employée par Leopoldt. Elle joue un rôle essentiel : en effet elle applique un groupe isomorphe à $W_m/W_{m/2}$ dans un groupe dont le 2-rang est égal au m -rang de $\mathcal{D}$. La différence : $\dim_m \mathcal{D} - \dim_m \overline{\mathcal{D}}$ est donc majorée par $\dim_2 \text{Ker } \theta_m$. Cette valeur est bornée au moyen d'un homomorphisme injectif ψ_m par $\dim_2 B^{**}/\pm B^{*2}$. Les définitions de ces ensembles : B^{**} et B^* sont données au paragraphe 2.

Dans le paragraphe 3, on majore cette dernière valeur par $n_1 + n_2 + n_3$. Ce calcul est élémentaire.

Le paragraphe 4 est consacré à l'énoncé d'inégalités qui bornent la différence $\dim_m \mathcal{H}_k - \dim_m \mathcal{H}_{k'}/j'(\mathcal{H}_k)$; k' désignant le corps $k(\sqrt{-1})$ et j' l'application canonique de $\mathcal{H}_k$ dans $\mathcal{H}_{k'}$.

Le paragraphe 5 contient quelques illustrations numériques.

Ces résultats n'auraient pas été mis en évidence sans les conseils et les encouragements de G. Gras. Je le prie de trouver ici l'expression de mes remerciements.

1. Définitions et rappels.

On désignera par k un corps de nombres et d un élément de k . Nous supposons qu'aucune des racines carrées $\sqrt{d}$, $\sqrt{-d}$, $\sqrt{-1}$ n'appartient à k . On notera m_0 la plus grande puissance de 2 telle que le sous-corps réel maximal $\mathbf{Q}_0^{(m_0)}$ du $m_0^{\text{ème}}$ corps cyclotomique soit inclus dans k et on désignera par ξ une racine primitive $m_0^{\text{ème}}$ de l'unité.

Nous poserons $K = k(\sqrt{d})$, $\bar{K} = k(\sqrt{-d})$, $k' = k(\sqrt{-1})$ et $L = k(\sqrt{d}, \sqrt{-d})$. Le groupe de Galois de L/k est un groupe de Klein que l'on désignera par G . L'élément de G qui laisse invariant K (resp. $\bar{K}$) sera noté σ (resp. $\bar{\sigma}$). Le groupe G est donc égal à $\{1, \sigma, \bar{\sigma}, \sigma\bar{\sigma}\}$. On a aussi $\xi^\sigma = \xi^{\bar{\sigma}} = \xi^{-1}$ et $k' = k(\xi)$.

Nous désignerons par ρ (resp. $\bar{\rho}$) la restriction de $\bar{\sigma}$ (resp. σ) à K (resp. $\bar{K}$). On a donc $\text{Gal}(K/k) = \{1, \rho\}$ et $\text{Gal}(\bar{K}/k) = \{1, \bar{\rho}\}$.

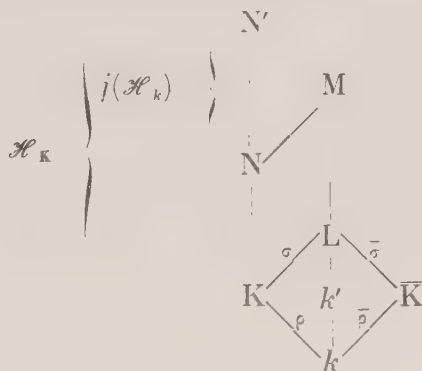
Nous désignerons par $\mathcal{H}_K, \mathcal{H}_{\bar{K}}, \mathcal{H}_k$ les 2-groupes des classes d'idéaux au sens restreint de $K, \bar{K}$ et k . Soient j et $\bar{j}$ les applications de $\mathcal{H}_k$ dans $\mathcal{H}_K$ et $\mathcal{H}_{\bar{K}}$ déduites des injections du groupe des idéaux de k dans les groupes d'idéaux de K et $\bar{K}$.

Nous poserons $\mathcal{D} = \mathcal{H}_K/j(\mathcal{H}_k)$ et $\bar{\mathcal{D}} = \mathcal{H}_{\bar{K}}/\bar{j}(\mathcal{H}_k)$.

Nous désignerons par N' la 2-extension abélienne, non ramifiée, maximale de K . (On entend par extension non ramifiée une extension dans laquelle aucun idéal ne se ramifie).

Rappelons que les deux groupes $\text{Gal}(N'/K)$ et $\mathcal{H}_K$ se correspondent dans l'isomorphisme de réciprocité. Cet isomorphisme est un isomorphisme de $\text{Gal}(K/k)$ -modules. (La structure de $\text{Gal}(K/k)$ -module de $\text{Gal}(N'/K)$ est définie par $y^c = r^{-1}yr$, r étant un prolongement de ρ à N' et y un élément de $\text{Gal}(N'/K)$). Composant cet isomorphisme avec la correspondance classique de Galois, on en déduit une bijection canonique entre les sous- $\text{Gal}(K/k)$ -modules de $\mathcal{H}_K$ et les sous-corps de N' , contenant K et galoisiens sur k . Désignons par N le sous-corps de N' qui correspond ainsi à $j(\mathcal{H}_K)$. Le groupe de Galois : $\text{gal}(N/K)$ est isomorphe à $\mathcal{D}$ et la structure de $\text{Gal}(K/k)$ -module de $\text{Gal}(N/K)$ est donc déterminée par $y^c = y^{-1}$, pour tout y de $\text{Gal}(N/K)$.

Posons encore $M = NL$. Suivant que L soit inclus dans N ou non, on aura $M = N$ ou $[M:N] = 2$. Le dessin suivant résume les notations introduites :



Dans toute la suite on désignera par m une puissance de 2. Si H est un F_2 -espace vectoriel, on notera $\dim_2 H$ sa dimension. Si H est un 2-groupe abélien, on notera $\dim_m H$ son m -rang, c'est-à-dire : $\dim_m H = \dim_2 H^{m/2}/H^m$. Si l'on décompose H en produit direct de groupes cycliques, $\dim_m H$ est le nombre de composantes de H d'ordre supérieur ou égal à m . On notera $H^{(m)}$ l'ensemble des éléments de H dont la puissance m^{eme} est égale à 1. On a :

$$\dim_2 H^{(m)}/H^{(m/2)} = \dim_m H.$$

Désormais, on désigne par m une puissance de 2 inférieure à m_0 . Soit N_m le corps intermédiaire entre N et K , maxi-

mal tel que N_m/K soit d'exposant divisant m . Nous avons donc :

$$\text{Gal}(N_m/K) \cong \mathcal{D}/\mathcal{D}^m.$$

Posons $M_m = N_m L$.

L'extension M_m/L est une extension de Kummer dont le radical sera désigné par W_m . On a donc $W_m = \{\omega; \omega \in M_m, \omega^m \in L^*\}$, et pour tout m compris entre 4 et m_0 :

$$\begin{aligned} \dim_m \mathcal{D} &= \dim_2 \text{Gal}(N_m/N_{m/2}) = \dim_2 \text{Gal}(M_m/M_{m/2}) \\ &= \dim_2 W_m/W_{m/2}. \end{aligned}$$

Nous avons de plus besoin d'une structure de G-module sur les groupes W_m/L^* . Si τ est un élément de G , on note t un prolongement de τ à M_m . Si ω appartient à W_m , l'élément $\omega^t L^*$ de W_m/L^* ne dépend pas du choix de t mais seulement de τ . En posant $(\omega L^*)^\tau = \omega^t L^*$, on définit sur W_m/L^* une structure de G-module. D'autre part, munissons $\text{Gal}(M_m/L)$ de la structure de G-module ainsi définie : Pour tout y de $\text{Gal}(M_m/L)$, $y^\tau = t^{-1} y t$.

Nous aurons alors $y^{\bar{\sigma}} = y^{-1}$ et $y^\tau = y$.

Désignons par $\text{Gal}(M_m/L)^\wedge$ le dual de $\text{Gal}(M_m/L)$ c'est-à-dire le groupe des homomorphismes de $\text{Gal}(M_m/L)$ dans L^* . Rappelons que la théorie de Kummer donne un isomorphisme canonique de W_m/L^* sur $\text{Gal}(M_m/L)^\wedge$ ainsi défini : si ωL^* appartient à W_m/L^* , il lui correspond $\alpha(\omega L^*)$ qui est l'homomorphisme de $\text{Gal}(M_m/L)$ dans L^* défini par : $\alpha(\omega L^*)(y) = \omega^{y-1}$.

Écrivons cette égalité avec y^τ : nous aurons donc :

$$\alpha(\omega L^*)(y^\tau) = \omega^{t^{-1} y t - 1}.$$

Écrivons-la également avec $(\omega L^*)^\tau$ et y .

Comme τ est d'ordre 2, on aura :

$$\alpha((\omega L^*)^\tau)(y) = (\omega^{t^{-1}})^{y-1}; \quad \text{d'où :} \quad \alpha((\omega L^*)^\tau)(y)^\tau = \omega^{t^{-1} y t - 1}.$$

Nous en déduisons : $\alpha((\omega L^*)^\tau)(y)^\tau = \alpha(\omega L^*)(y^\tau)$. Cette quantité est une racine $m_0^{\text{ème}}$ de 1 et nous avons vu que $\zeta^\sigma = \zeta^{\bar{\sigma}} = \zeta^{-1}$. Faisons $\tau = \sigma$ dans la relation précédente. Nous obtenons : $\alpha((\omega L^*)^\sigma) = \alpha(\omega L^*)^{-1}$ d'où $(\omega L^*)^\sigma = (\omega L^*)^{-1}$. D'autre part, en remplaçant τ par $\bar{\sigma}$, dans la même relation, on obtient $(\omega L^*)^{\bar{\sigma}} = \omega L^*$.

Remarque. — Nous venons de redémontrer ce que Leopoldt appelle plus généralement « Spiegelungsrelation » [4].

Résumons les résultats obtenus dans la

PROPOSITION 1. — Soit m une puissance de 2 inférieure à m_0 et soit N_m le corps intermédiaire entre N et K maximal tel que N_m soit d'exposant divisant m . Soit $M_m = N_m L$ et soit W_m le radical de M_m .

(i) La structure de G -module de W_m/L^* est déterminée par les relations: $(\omega L^*)^\sigma = (\omega L^*)^{-1}$ et $(\omega L^*)^{\bar{\sigma}} = \omega L^*$.

(ii) Si de plus m est supérieur ou égal à 4,

$$\dim_m \mathcal{D} = \dim_2 W_m / W_{m/2}.$$

2. Applications θ_m et ψ_m .

PROPOSITION 2a. — L'extension N/K est décomposée sur k et l'extension M/L est décomposée sur K .

Démonstration. — Rappelons d'abord que l'extension N/K est dite décomposée sur k lorsque $\text{Gal}(N/k)$ est produit semi-direct de l'un de ses sous-groupes par $\text{Gal}(N/K)$. Il revient au même de dire qu'il existe un sous-corps X de N tel que: $N = KX$ et $K \cap X = k$.

Soit r un prolongement de ρ à N' et soient $\langle r \rangle$ et $\langle r^2 \rangle$ les sous-groupes de $\text{Gal}(N'/k)$ engendrés par r et r^2 . Ce dernier sous-groupe est inclus dans le centre de $\text{Gal}(N'/k)$. Si N_0 est le sous-corps de N laissé invariant par $\langle r^2 \rangle$, l'extension N_0/k est donc galoisienne. De plus on a:

$$\text{Gal}(N'/N_0) = \langle r^2 \rangle = \text{Gal}(N'/K) \cap \langle r \rangle,$$

et

$$\text{Gal}(N'/k) = \text{Gal}(N'/K) \langle r \rangle.$$

L'extension N_0/K est donc décomposée sur k .

Montrons maintenant que N_0 contient N . D'après la théorie du corps des classes, il existe un idéal $\mathfrak{P}$ de N' , non ramifié dans N'/k , tel que r soit égal à l'automor-

phisme de Frobenius $(\mathfrak{P}, N'/k)$. Soit $\mathfrak{p}$ l'idéal premier de K en dessous de $\mathfrak{P}$. Si f est le degré résiduel de $\mathfrak{p}$ dans K/k , nous aurons $r^f = (\mathfrak{P}, N'/K)$; d'où $f = 2$. D'autre part, N'/K est abélienne, le symbole $(\mathfrak{P}, N'/K)$ ne dépend plus que de $\mathfrak{p}$ et nous pouvons écrire $r^2 = (\mathfrak{p}, N'/K)$. Puisque $f = 2$, $\mathfrak{p}$ est l'étendu d'un idéal premier de k . Dans l'isomorphisme de réciprocity liant $\text{Gal}(N'/K)$ et $\mathcal{H}_K$, r^2 est donc l'image d'une classe d'idéaux appartenant à $j(\mathcal{H}_k)$. Le corps N_0 contient donc N et puisque N_0/K est décomposée sur k , il en sera de même de N/K .

Il reste à voir que cette propriété de décomposition se transmet à M/L . Si $N \cap L = K$, les groupes de Galois $\text{Gal}(M/\bar{K})$ et $\text{Gal}(N/k)$ sont isomorphes par restriction des automorphismes de M à N . Dans cet isomorphisme, $\text{Gal}(N/K)$ correspond à $\text{Gal}(M/L)$ et l'extension M/L sera décomposée sur $\bar{K}$. Supposons maintenant que L soit contenu dans N . Nous avons alors $M = N$. Désignons désormais par r un prolongement d'ordre 2 de ρ à N et par s un prolongement de σ à N . L'automorphisme r prolonge donc $\bar{\sigma}$ ou $\sigma\bar{\sigma}$, et r ou rs est un prolongement de $\bar{\sigma}$ à M .

Calculons $(rs)^2$. Comme $rsr = r^{-1}sr = s^{-1}$, on en déduit $(rs)^2 = 1$. Le groupe $\text{Gal}(M/\bar{K})$ est donc produit semi-direct de $\text{Gal}(M/L)$ par l'un ou l'autre des sous-groupes $\{1, r\}$ ou $\{1, rs\}$. L'extension M/L est donc décomposée sur $\bar{K}$.

Remarque. — La première assertion de cette proposition pouvait être remplacée par l'énoncé plus général suivant : " Si K/k est une extension cyclique de degré quelconque; si $\mathcal{H}_K$ et $\mathcal{H}_k$ sont les groupes des classes de K et k ; si j est l'application canonique de $\mathcal{H}_k$ dans $\mathcal{H}_K$; si N est le sous-corps du corps des classes de Hilbert N' de K , correspondant à $j(\mathcal{H}_k)$, c'est-à-dire invariant par l'image de $j(\mathcal{H}_k)$ dans l'isomorphisme de réciprocity : $\text{Gal}(N'/K) \cong \mathcal{H}_K$, alors l'extension N/K est décomposée sur k ". La démonstration est semblable à celle donnée plus haut.

DÉFINITION DE W'_m . — Nous désignerons désormais par $\bar{s}$ un prolongement de $\bar{\sigma}$ à M , d'ordre 2. Pour toute puissance de 2 notée m et inférieure à m_0 , nous noterons W'_m l'ensemble des éléments de W_m invariants par $\bar{s}$.

PROPOSITION 2b. — L'injection canonique de W'_m dans W_m induit un isomorphisme de $W'_m/\bar{K}^*$ sur W_m/L^* . De plus, quel que soit ω de W'_m , $\omega^{m(\sigma+1)}$ appartient à k^m .

Démonstration. — Considérons l'application de W'_m dans W_m/L^* qui associe à tout ω' de W'_m , $\omega'L^*$. Si ω est un élément de W_m , alors compte tenu de la proposition 1 (i), $\omega^{\bar{s}-1}$ appartient à L . Comme $\bar{s}$ est d'ordre 2, on en déduit : $(\omega^{\bar{s}-1})^{\bar{s}+1} = 1$, et il existe α dans L tel que $\omega^{\bar{s}-1} = \alpha^{\bar{s}-1}$. Posons alors $\omega' = \omega\alpha^{-1}$. On a $\omega L^* = \omega' L^*$ et ω' appartient à W'_m . L'application considérée est donc surjective. On en déduit l'isomorphisme annoncé.

Soit maintenant ω un élément de W'_m . Il est nécessaire de distinguer deux cas :

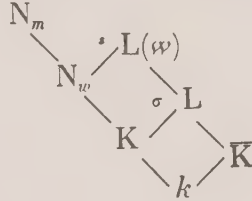
Premier cas : Il existe un sous-corps N_w de N_m tel que $L(\omega) = N_w L$ et $N_w \cap L = K$. Désignons alors par s un prolongement de σ à $L(\omega)$ qui invarie N_w . Désignons encore par $\bar{s}$ la restriction de $\bar{s}$ à $L(\omega)$. On a :

$$L(\omega) = N_w \bar{K} \quad \text{et} \quad N_w \cap \bar{K} = k.$$

On en déduit $s^2 = \bar{s}^2 = 1$ et $s\bar{s} = \bar{s}s$.

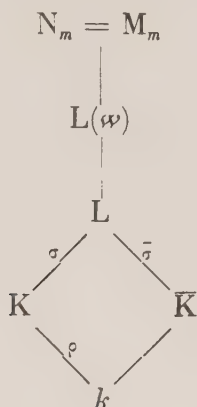
En vertu de la proposition 1, ω^{s+1} appartient à L . De plus ω^{s+1} est invariant par σ et $\bar{\sigma}$. Donc il appartient à k .

On en déduit que $\omega^{m(\sigma+1)}$ appartient à k^m .



Deuxième cas : Il n'existe pas de sous-corps N_w de N_m tel que $L(\omega) = LN_w$ et $L \cap N_w = K$. Dans ce cas, on aura donc : $L \subset N$, $N = M$ et $N_m = M_m$. Désignons encore par $\bar{s}$ la restriction de $\bar{s}$ à $L(\omega)$ et par s un prolongement de σ à $L(\omega)$. Comme $\bar{s}$ est un prolongement de ρ , nous avons $s^\rho = \bar{s}s\bar{s} = s^{-1}$. On posera $\zeta_m = \zeta_{m_0/m}$. Soit m' l'expo-

sant de $L(\varpi)/K$. Si les exposants de $\text{Gal}(L(\varpi)/K)$ et $\text{Gal}(L(\varpi)/L)$ étaient égaux et puisque $\text{Gal}(L(\varpi)/L)$ est cyclique, alors $\text{Gal}(L(\varpi)/L)$ serait facteur direct de $\text{Gal}(L(\varpi)/K)$ et $L(\varpi)/L$ se décomposerait sur K . Ces deux exposants sont donc différents et cela prouve que $L(\varpi)/K$ est cyclique de degré m' . De plus s engendre le groupe de Galois de cette extension. Si $m' = 2$, ϖ appartient à $\bar{K}$ et on obtient tout de suite le résultat. Supposons maintenant $m' \geq 4$ et montrons que ϖ^{1+s} appartient à $\zeta_m^{-1}K$.



L'extension $L(\varpi)/L$ est une extension de Kummer de degré $m'/2$ dont le groupe de Galois est engendré par s^2 .

On aura donc : $\varpi^{s^2} = \zeta_{m'/2}\varpi$ et $\varpi^{(1+s)s} = \zeta_{m'/2}\varpi^{1+s}$. Or 1 et ζ_m^{-1} forment une base de L/K . Il suffit de décomposer ϖ^{1+s} sur cette base pour constater que ϖ^{1+s} appartient à $\zeta_m^{-1}K$. De plus, on a $\varpi^{1+s} = \varpi^{1+\bar{s}s}$. On en déduit que ϖ^{1+s} est invariant par $\bar{s}s$. Cela prouve que ϖ^{1+s} appartient à k' . Comme $\zeta_m^{-1}K \cap k' = \zeta_m^{-1}k$, on en déduit que $\varpi^{(1+s)m'}$ appartient à $k^{m'}$. Puisqu'enfin, $L(\varpi)$ est inclus dans $M_m = N_m$, m' divise m et $\varpi^{m(1+s)}$ appartient à k^m .

Désignons par A_k , A_L et $A_{\bar{K}}$ les anneaux d'entiers de k , L et $\bar{K}$.

LEMME 2a. — Si m est une puissance de 2 comprise entre 2 et m_0 et si ϖ appartient à W'_m , alors ϖ^m appartient à $\bar{K}$ et l'idéal engendré par ϖ^m est de la forme $\varpi^m A_{\bar{K}} = \mathbb{C}^{m/2} \mathfrak{A}^m$; $\mathbb{C}$ étant un idéal de k et $\mathfrak{A}$ un idéal de $\bar{K}$.

Démonstration. — Supposons donc que ω appartienne à W'_m . L'extension $L(\omega)/L$ est non ramifiée d'exposant divisant m et l'idéal $\omega^m A_L$ est donc la puissance m^{eme} d'un idéal de L . Écrivons cet idéal sous la forme $\mathfrak{B}\mathfrak{D}$, $\mathfrak{B}$ étant un idéal de L ramifié dans $L/\bar{K}$ et $\mathfrak{D}$ un idéal de L non ramifié dans $L/\bar{K}$. On a donc $\omega^m A_L = \mathfrak{B}^m \mathfrak{D}^m$. Comme ω^m appartient à $\bar{K}$, nous aurons $\mathfrak{D}^{\bar{\sigma}} = \mathfrak{D}$ et $\mathfrak{D}$ est l'étendu d'un idéal de $\bar{K}$. Quant à $\mathfrak{B}$, on peut le décomposer en produit d'idéaux premiers (ramifiés sur $\bar{K}$) de la façon suivante :

$$\mathfrak{B} = \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_2^{a_2} \dots \mathfrak{p}_3^{a_3 + \sigma a'_3} \dots,$$

avec :

- $\mathfrak{p}_1$ idéal de L complètement ramifié dans L/k ;
- $\mathfrak{p}_2$ idéal de L ramifié dans $L/\bar{K}$ et inerte dans L/K ;
- $\mathfrak{p}_3$ idéal de L ramifié dans $L/\bar{K}$ et décomposé dans L/K .

D'après la proposition 2b, $\omega^{m(1+\sigma)}$ appartient à k^m et d'autre part $\mathfrak{D}^{\sigma+1}$ est l'étendu d'un idéal de k . Donc,

$$\mathfrak{B}^{\sigma+1} = \mathfrak{p}_1^{2a_1} \dots \mathfrak{p}_2^{2a_2} \dots \mathfrak{p}_3^{(a_3 + a'_3)(1+\sigma)} \dots$$

est aussi l'étendu d'un idéal de k . On aura donc $a_1 \equiv 0 \pmod{2}$ et $a_3 + a'_3 \equiv 0 \pmod{2}$. On en déduit que $\mathfrak{p}_1^{a_1}$ est l'étendu d'un idéal de $\bar{K}$. Si a_3 est pair, $\mathfrak{p}_3^{a_3}$ est l'étendu d'un idéal de $\bar{K}$ et il en est de même de $\mathfrak{p}_3^{\sigma a'_3}$. Si maintenant a_3 est impair, on peut écrire :

$$\mathfrak{p}_3^{a_3 + \sigma a'_3} = \mathfrak{p}_3^{a_3 - 1 + \sigma(a'_3 - 1)} \mathfrak{p}_3^{1 + \sigma} \quad \text{et} \quad \mathfrak{p}_3^{2(1 + \sigma)}$$

est l'étendu d'un idéal de k . Finalement $\mathfrak{p}_3^{(a_3 + \sigma a'_3)m}$ sera l'étendu d'un idéal de $\bar{K}$ de la forme $\mathfrak{G}^{m/2} \mathfrak{A}^m$, $\mathfrak{G}$ étant un idéal de k et $\mathfrak{A}$ un idéal de $\bar{K}$. Quant à $\mathfrak{p}_2$, il est tel que $\mathfrak{p}_2^2$ soit l'étendu d'un idéal de k . Donc $\mathfrak{p}_2^m$ est l'étendu d'un idéal de la forme $\mathfrak{G}^{m/2}$, $\mathfrak{G}$ étant un idéal de k . Nous avons donc montré que $\omega^m A_L = \mathfrak{G}^{m/2} \mathfrak{A}^m A_L$, avec $\mathfrak{G}$ idéal de k et $\mathfrak{A}$ idéal de $\bar{K}$. Comme ω^m appartient à $\bar{K}$, on en déduit : $\omega^m A_K = \mathfrak{G}^{m/2} \mathfrak{A}^m$.

PROPOSITION 2c. — Soit m une puissance de 2 comprise entre 2 et m_0 . Si ω appartient à W'_m , soit $Cl(\mathfrak{A})$ la

classe de l'idéal $\mathfrak{A}$ de $\bar{K}$ défini par le lemme 2a. Alors $\text{Cl}(\mathfrak{A})^m$ appartient à $\bar{j}(\mathcal{H}_k)$.

Démontrons tout d'abord le lemme suivant :

LEMME 2b. — Soit x un élément de $\bar{K}$, tel que $x^{\sigma+1}$ soit un élément totalement positif de k . Alors il existe c dans k tel que xc soit un élément totalement positif de $\bar{K}$.

En effet, on peut écrire les plongements réels de $\bar{K}$ dans $\mathbf{C}$ sous la forme $p_1, \dots, p_s, \sigma p_1, \dots, \sigma p_s$ et les restrictions de $p_1, \dots, p_s$ à k seront des plongements distincts de k dans $\mathbf{C}$.

Soit c un élément de k tel que c^{p_i} ait le même signe que x^{p_i} , pour tout i de 1 à s . Nous aurons donc $(xc)^{p_i} > 0$ et $(xc)^{\sigma p_i} > 0$. Ceci montre que xc est un élément totalement positif de $\bar{K}$.

Démontrons la proposition 2c. Soit ω un élément de W'_m . En vertu de la proposition 1 (ii), du lemme 2b et puisque m est supérieur à 2, il existe c dans k tel que $\omega^m c^{-1}$ soit totalement positif.

Nous en déduisons : $\text{Cl}(\omega^m A_{\bar{K}}) = \text{Cl}(c A_{\bar{K}})$. (Il n'est question ici que de classes au sens restreint). D'où $\text{Cl}(\omega^m A_{\bar{K}})$ appartient à $\bar{j}(\mathcal{H}_k)$. Comme $\omega^m A_{\bar{K}} = \mathfrak{G}^{m/2} \mathfrak{A}^m$, avec $\mathfrak{A}$ idéal de k , on en déduit que $\text{Cl}(\mathfrak{A})^m$ appartient à $\bar{j}(\mathcal{H}_k)$. En d'autres termes, $\text{Cl}(\mathfrak{A}) \bar{j}(\mathcal{H}_k)$ appartient à $\overline{\mathcal{D}}^{(m)}$. On en déduit la définition de θ_m .

DÉFINITION DE θ_m . — Soit m une puissance de 2 comprise entre 4 et m_0 . Soit ω appartenant à W'_m et soit $\text{Cl}(\mathfrak{A})$ la classe de l'idéal $\mathfrak{A}$ de $\bar{K}$ défini par le lemme 2a. Nous noterons θ_m l'homomorphisme de $W'_m / W'_{m/2}$ dans $\overline{\mathcal{D}}^{(m)} / \overline{\mathcal{D}}^{(m/2)}$ qui associe à $\omega W'_{m/2}$ la classe de $\text{Cl}(\mathfrak{A}) \bar{j}(\mathcal{H}_k)$ modulo $\overline{\mathcal{D}}^{(m/2)}$.

DEFINITION DE B^{**} ET B^* . — Nous désignerons par B^{**} l'ensemble des éléments u de $\bar{K}$ tels que l'idéal engendré par u soit de la forme $\mathfrak{G}^2 b^2 A_{\bar{K}}$ avec $\mathfrak{G}$ idéal de k , b élément totalement positif de $\bar{K}$, et tels que $u^{\sigma+1}$ appartienne à k^4 .

En abrégé :

$$B^{**} = \{u; u \in \bar{K}, uA_{\bar{K}} = \mathfrak{G}^2 b^2 A_{\bar{K}}, \mathfrak{G} \text{ idéal de } k, b \in \bar{K}^+, u^{\sigma+1} \in k^4\}.$$

Nous noterons B^* , l'ensemble des éléments de $\bar{K}$, dont la norme dans $\bar{K}/k$ est un carré de k . En abrégé :

$$B^* = \{u; u \in \bar{K}, u^{\sigma+1} \in k^2\}.$$

On déduit immédiatement du lemme 2b, que B^{*2} est inclus dans B^{**} .

DÉFINITION DE ψ_m . — Soit m une puissance de 2 comprise entre 4 et m_0 . Supposons que $\omega W'_{m/2}$ appartienne à $\text{Ker } \theta_m$. Conservons les notations du lemme 2a, c'est-à-dire : $\omega^m A_{\bar{K}} = \mathfrak{G}^{m/2} \mathfrak{A}^m$. Nous avons donc : $\text{Cl}(\mathfrak{A})^{m/2}$ appartient à $\bar{j}(\mathcal{H}_k)$ et il existe un idéal $\mathfrak{G}_0$ de k et un élément b totalement positif de $\bar{K}$ tels que

$$\mathfrak{A}^{m/2} = \mathfrak{G}_0 b A_{\bar{K}}; \quad \text{d'où} \quad \omega^m A_{\bar{K}} = \mathfrak{G}^{m/2} \mathfrak{G}_0^2 b^2 A_{\bar{K}}.$$

D'autre part, en vertu de la proposition 1 (ii), $\omega^{m(\sigma+1)}$ appartient à k^4 . Nous avons donc vérifié que ω^m appartient à B^{**} .

Supposons maintenant que ω appartienne à $W'_{m/2}$; alors $\omega^{(m/2)(\sigma+1)}$ appartient à k^2 , $\omega^{m/2}$ appartient à B^* et ω^m appartient à B^{*2} . Il s'en suit que l'on peut définir un homomorphisme ψ_m de $\text{Ker } \theta_m$ dans $B^{**}/\pm B^{*2}$ en associant à l'élément $\omega W'_{m/2}$ de $\text{ker } \theta_m$, la classe de ω^m modulo $\pm B^{*2}$.

PROPOSITION 2d. — L'homomorphisme ψ_m défini ci-dessus est injectif.

Démonstration. — Supposons que $\omega W'_{m/2}$ appartienne à $\text{Ker } \theta_m$. Cela signifie que ω^m appartient à $\pm B^{*2}$. On en déduit d'abord que ω^m appartient à L^2 et que $L(\omega)/L$ est d'exposant divisant $m/2$. Nous aurons $\omega^{m/2} = u$ ou $\sqrt{-1}u$ avec u dans B^* . On en déduit aussi que $\omega^{(m/2)(\sigma+1)}$ appartient à k^2 . Ceci montre que $L(\omega^{m/4})/L$ est décomposée sur K , c'est-à-dire que $L(\omega^{m/4})/K$ est d'exposant 2.

(En vertu du critère de décomposition classique des extensions biquadratiques). L'extension $L(\varpi)/K$ est donc d'exposant divisant $m/2$ et ϖ appartient à $M_{m/2}$, donc à $W_{m/2}$.

Remarque. — On peut définir une application de $W'_m/W'_{m/2}$ dans $W'_{m/2}/W'_{m/4}$ en associant à $\varpi W'_{m/2}$, $\varpi^2 W'_{m/4}$. Il s'agit d'un homomorphisme injectif. De plus si $\varpi W'_{m/2}$ appartient à $\text{Ker } \theta_m$, alors $\varpi^2 W'_{m/4}$ appartient à $\text{Ker } \theta_{m/2}$. Pour toute puissance de 2 comprise entre 8 et m_0 , il existe donc un homomorphisme injectif β_m de $\text{Ker } \theta_m$ dans $\text{Ker } \theta_{m/2}$. On a d'ailleurs $\psi_m = \psi_{m/2} \circ \beta_m$.

Le corollaire suivant se déduit des propositions précédentes :

COROLLAIRE. — *Pour toute puissance de 2 notée m et comprise entre 4 et m_0 , on a :*

$$\dim_m \mathcal{D} - \dim_m \overline{\mathcal{D}} \leq \dim_2 B^{**} / \pm B^{*2}.$$

En effet, $\dim_m \mathcal{D}$ est égal à $\dim_2 W'_m/W'_{m/2}$ en vertu des propositions 1 et 2b. D'autre part, $\dim_m \overline{\mathcal{D}} = \dim_2 \overline{\mathcal{D}}^{(m)} / \overline{\mathcal{D}}^{(m/2)}$. En factorisant l'homomorphisme θ_m , on obtient l'inégalité :

$$\dim_2 W'_m/W'_{m/2} - \dim_2 \overline{\mathcal{D}}^{(m)} / \overline{\mathcal{D}}^{(m/2)} \leq \dim_2 \text{Ker } \theta_m,$$

c'est-à-dire :

$$\dim_m \mathcal{D} - \dim_m \overline{\mathcal{D}} \leq \dim_2 \text{Ker } \theta_m.$$

Enfin, on déduit de la proposition 2d l'inégalité :

$$\dim_2 \text{Ker } \theta_m \leq \dim_2 B^{**} / \pm B^{*2}.$$

3. Majoration de $B^{**} / \pm B^{*2}$.

Notations. — On désignera par $E_{\overline{K}}$ (resp. E_k) le groupe des unités de $\overline{K}$ (resp. k). Les dimensions sur $\mathbf{Z}$ des groupes quotients de ces groupes par leurs sous-groupes de torsion seront notés $\dim_{\mathbf{Z}}(E_{\overline{K}})$ et $\dim_{\mathbf{Z}}(E_k)$. L'ensemble des éléments totalement positifs de $\overline{K}$ (resp. k) sera noté $\overline{K}^+$ (resp. k^+). On posera également $E_{\overline{K}}^+ = E_{\overline{K}} \cap \overline{K}^+$ et $E_k^+ = E_k \cap k^+$. Dans ce paragraphe, on notera N au lieu de $N_{\overline{K}/k}$, la norme dans l'extension $\overline{K}/k$.

On désignera par E^{**} (resp. E^*) l'ensemble des unités ε de $\bar{K}$ telles que $N(\varepsilon)$ appartienne à k^4 (resp. k^2). En abrégé :

$$\begin{aligned} E^{**} &= E_{\bar{K}} \cap B^{**} = \{\varepsilon; \varepsilon \in E_{\bar{K}}, \varepsilon^{\sigma+1} \in k^4\} \\ E^* &= E_{\bar{K}} \cap B^* = \{\varepsilon; \varepsilon \in E_{\bar{K}}, \varepsilon^{\sigma+1} \in k^2\}. \end{aligned}$$

On notera F (resp. F') l'ensemble des éléments de $\bar{K}$ engendrant un idéal qui est l'étendu d'un idéal de k (resp. d'un idéal strictement principal de k). En abrégé :

$$\begin{aligned} F &= \{u; u \in \bar{K}, uA_{\bar{K}} = \mathfrak{G}A_{\bar{K}}, \mathfrak{G} \text{ idéal de } k\} \\ F' &= \{u; u \in \bar{K}, uA_{\bar{K}} = \mathfrak{G}A_{\bar{K}}, \mathfrak{G} \text{ idéal strict. principal de } k\}. \end{aligned}$$

On a donc $F' = k^+E_{\bar{K}}$. On posera aussi :

$$F^+ = \bar{K}^+ \cap F \quad \text{et} \quad F'^+ = \bar{K}^+ \cap F'.$$

On notera C (resp. C') l'ensemble des éléments de k engendrant le carré d'un idéal de k (resp. le carré d'un idéal principal au sens ordinaire de k). En abrégé :

$$\begin{aligned} C &= \{u; u \in k, uA_k = \mathfrak{G}^2, \mathfrak{G} \text{ idéal de } k\} \\ C' &= \{u; u \in k, uA_k = \mathfrak{G}^2, \mathfrak{G} \text{ idéal principal ordinaire de } k\}. \end{aligned}$$

On a donc $C' = k^2E_k$.

Nous noterons P_k le sous-groupe de $\mathcal{H}_k$ engendré par les classes d'idéaux principaux (au sens ordinaire) de k . Enfin nous définirons les constantes n_1, n_2, n_3 en posant :

$$\begin{aligned} n_1 &= \dim_{\mathbb{Z}} E_{\bar{K}} - \dim_{\mathbb{Z}} E_k \\ n_2 &= \dim_2 (E_k^+ \cap N\bar{K})/E_k^2 N E_{\bar{K}}^+ \\ n_3 &= \dim_2 \mathcal{H}_k^{(2)}/\text{Ker } \bar{j} P_k. \end{aligned}$$

PROPOSITION 3a. — *Il existe une suite exacte :*

$$1 \rightarrow B^{*2}E^{**}/\pm B^{*2} \rightarrow B^{**}/\pm B^{*2} \xrightarrow{f} C \cap N\bar{K}^+/k^2NF^+.$$

Démonstration. — Définissons tout d'abord l'application f . Si u appartient à B^{**} , il engendre un idéal de la forme : $uA_{\bar{K}} = \mathfrak{G}^2 b^2 A_{\bar{K}}$ avec $\mathfrak{G}$ idéal de k et b dans $\bar{K}^+$. De plus, on a $u^{\sigma+1} = v^4$ avec v dans k . D'où :

$$v^2 A_k = \mathfrak{G}^2 b^{\sigma+1} A_k.$$

Nous définissons $f(u)$ comme étant la classe de $\nu^2 b^{-(\sigma+1)}$ modulo $k^2 \text{NF}^+$.

Montrons qu'il s'agit bien d'une application. Rappelons d'abord que $k^+ \cap N\bar{K} = N\bar{K}^+$. Ceci prouve que $\nu^2 b^{-(\sigma+1)}$ appartient à $C \cap N\bar{K}^+$. Montrons que $f(u)$ ne dépend pas du choix de $\mathfrak{G}$ et b .

Si $uA_{\bar{K}}$ s'écrit de deux façons :

$$uA_{\bar{K}} = \mathfrak{G}^2 b^2 A_{\bar{K}} = \mathfrak{G}'^2 b'^2 A_{\bar{K}}$$

nous aurons alors :

$$bb'^{-1}A_{\bar{K}} = \mathfrak{G}'\mathfrak{G}^{-1}A_{\bar{K}} \quad \text{et} \quad bb'^{-1}$$

appartient à F^+ . D'où

$$\nu^2 b^{-(\sigma+1)}[\nu^2 b'^{-(\sigma+1)}]^{-1} = (bb'^{-1})^{-(\sigma+1)}$$

appartient à NF^+ et $f(u)$ ne dépend pas du choix de $\mathfrak{G}$ et b .

Supposons maintenant que u appartienne à $\pm B^{*2}$.

Nous pouvons alors (Lemme 2b) écrire un élément de B^* sous la forme cb avec c dans k et b dans $\bar{K}^+$. La quantité u est donc de la forme $u = \pm c^2 b^2$ et on a :

$$uA_{\bar{K}} = c^2 b^2 A_{\bar{K}}.$$

Définissons ν : On a

$$u^{\sigma+1} = c^4 b^{2(\sigma+1)} \quad \text{d'où} \quad \nu^4 = c^4 b^{2(\sigma+1)}$$

et

$$\nu^2 = \pm c^2 b^{\sigma+1}.$$

Mais $c^2 b^{\sigma+1}$ est un carré dans k et -1 ne peut être un carré dans k . On a donc $\nu^2 = c^2 b^{\sigma+1}$ et $f(u)$ est la classe modulo $k^2 \text{NF}^+$ de $\nu^2 b^{-(\sigma+1)} = c^2$. Donc $f(u)$ est égal à $k^2 \text{NF}^+$. Nous avons bien défini un homomorphisme f .

Montrons que $\text{Ker } f$ est inclus dans $B^{*2}E^{**}/\pm B^{*2}$. Conserverons les notations introduites au début de cette démonstration. Supposons que $u(\pm B^{*2})$ appartienne à $\text{Ker } f$. Il existe donc z dans F^+ et c dans k tels que $\nu^2 b^{-(\sigma+1)} = z^{\sigma+1} c^2$.

Nous aurons

$$\mathfrak{G}^2 = \nu^2 b^{-(\sigma+1)} A_k = z^{\sigma+1} c^2 A_k.$$

D'où :

$$uA_{\bar{K}} = \mathbb{G}^2 b^2 A_{\bar{K}} = z^{\sigma+1} c^2 b^2 A_{\bar{K}}.$$

Mais z appartient à F . Cela prouve que $z^{\sigma+1} A_{\bar{K}} = z^2 A_{\bar{K}}$ et nous aurons :

$$uA_{\bar{K}} = (zcb)^2 A_{\bar{K}} \quad \text{et} \quad u = (zcb)^2 \varepsilon$$

avec ε dans $E_{\bar{K}}$. Or $(zcb)^{\sigma+1} = \nu^2$ et zcb appartient à B^* . Donc ε appartient à E^{**} et u appartient à $B^{*2}E^{**}$.

L'inclusion inverse ne présente pas de difficulté. Si ε appartient à E^{**} , alors on a $\varepsilon A_{\bar{K}} = A_{\bar{K}}$ et on peut choisir pour calculer $f(\varepsilon)$: $\mathbb{G} = A_k$, $b = 1$. Il s'en suit que si $\varepsilon^{\sigma+1} = \nu^4$, $f(\varepsilon)$ est égal à $k^2 NF^+$.

PROPOSITION 3b.

$$\dim_2 B^{*2}E^{**}/\pm B^{*2} = \dim_2 E^{**}/\pm E^{*2} \leq n_1.$$

Démonstration. — La première égalité est immédiate. En effet :

$$B^{*2}E^{**}/\pm B^{*2} \cong E^{**}/\pm B^{*2} \cap E^{**} = E^{**}/\pm E^{*2}.$$

Comme $\sqrt{-1}$ n'appartient pas à $\bar{K}$, le 2-sous-groupe de torsion de E^{**} est ± 1 . D'autre part $E_{\bar{K}}^4$ est inclus dans E^{**} et cela prouve que $\dim_Z E^{**}$ est égal à $\dim_Z E_{\bar{K}}$. Nous aurons donc :

$$\dim_2 E^{**}/\pm E^{*2} = \dim_Z E_{\bar{K}}.$$

Le groupe des unités de k , E_k est inclus dans E^* . Considérons l'homomorphisme de E_k^2 dans E^{*2}/E^{**2} qui associe à α^2 (α appartenant à E_k), $\alpha^2 E^{**2}$. Il a pour noyau E_k^4 . Cela montre que :

$$\dim_2 E_k^2/E_k^4 \leq \dim_2 E^{*2}/E^{**2}.$$

Comme $\sqrt{-1}$ n'appartient pas à E_k , le 2-sous-groupe de torsion de E_k^2 est réduit à 1 et $\dim_2 E_k^2/E_k^4 = \dim_Z E_k$.

Enfin $\pm E^{*2}/\pm E^{**2} \cong E^{*2}/E^{**2}$ et on aura :

$$\begin{aligned} \dim_2 E^{**}/\pm E^{*2} &= \dim_2 E^{**}/\pm E^{**2} - \dim_2 \pm E^{*2}/\pm E^{**2} \\ &\leq \dim_Z E_{\bar{K}} - \dim_Z E_k = n_1. \end{aligned}$$

PROPOSITION 3c. — $\text{Dim}_2 C \cap N\bar{K}^+/k^2NF^+ \leq n_2 + n_3$.

La démonstration de cette inégalité repose sur l'existence d'un isomorphisme :

$$C' \cap N\bar{K}^+/k^2NF'^+ \cong E_k^+ \cap N\bar{K}/E_k^2NE_{\bar{K}}^+,$$

et de deux suites exactes :

$$\begin{aligned} 1 \rightarrow C' \cap N\bar{K}^+ &\rightarrow C \cap N\bar{K}^+ \rightarrow \mathcal{H}_k^{(2)}/P_k, \\ k^2NF^+/k^2NF'^+ &\rightarrow \text{Ker } \bar{j}/P_k \cap \text{Ker } \bar{j} \rightarrow 1. \end{aligned}$$

Considérons l'inclusion $E_k^+ \cap N\bar{K} \subset C' \cap N\bar{K}^+$ et l'application naturelle $f: E_k^+ \cap N\bar{K} \rightarrow C' \cap N\bar{K}^+/k^2NF'^+$. Soit ε un élément de $E_k^+ \cap N\bar{K}$ tel que ε appartienne à $k^2NF'^+$. Nous aurons donc : $\varepsilon = u^{\sigma+1}c^2$, avec c dans k et u dans F'^+ . Cet élément s'écrit donc $u = c_0\alpha$ avec c_0 dans k^+ et α dans $E_{\bar{K}}$. Comme u est totalement positif, α l'est aussi. On a donc $\varepsilon = \alpha^{\sigma+1}(c_0c)^2$ et c_0c appartient à E_k . Finalement ε appartient à $E_k^2NE_{\bar{K}}^+$. Réciproquement, l'inclusion $E_k^2NE_{\bar{K}}^+ \subset k^2NF'^+$ ne pose pas de problème. Nous avons donc montré que le noyau de f est $E_k^2NE_{\bar{K}}^+$.

Montrons maintenant que f est surjective. Soit u appartenant à $C' \cap N\bar{K}^+$. Nous avons donc $u = \nu^{\sigma+1}$ avec ν dans $\bar{K}^+$ et $u = \varepsilon c^2$ avec ε dans E_k^+ et c dans k . On en déduit que $uk^2NF'^+ = \varepsilon k^2NF'^+$ et comme $\varepsilon = (\nu c^{-1})^{\sigma+1}$, ε appartient donc à $E_k^+ \cap N\bar{K}$. L'image de ε par f est $uk^2NF'^+$. L'isomorphisme est démontré.

Soit maintenant u appartenant à $C \cap N\bar{K}^+$. Il existe un idéal $\mathfrak{G}$ de k tel que $uA_k = \mathfrak{G}^2$. Comme u est totalement positif, la classe de $\mathfrak{G}$ appartient à $\mathcal{H}_k^{(2)}$ et en associant à u la classe de $\text{Cl}(\mathfrak{G})$ modulo P_k , nous obtenons un homomorphisme de $C \cap N\bar{K}^+$ dans $\mathcal{H}_k^{(2)}/P_k$ qui a pour noyau $C' \cap N\bar{K}^+$. Ceci démontre que la première suite est exacte.

Soit u un élément de k^2NF^+ . Il s'écrit $u = \nu^{\sigma+1}c^2$ avec ν dans F^+ et c dans k . On a donc $\nu A_{\bar{K}} = \mathfrak{G}A_{\bar{K}}$. La classe de $\mathfrak{G}$ appartient à $\text{Ker } \bar{j}$. Cette classe est définie modulo $P_k \cap \text{Ker } \bar{j}$. En effet si on écrit $u = \nu'^{\sigma+1}c'^2$ avec ν' dans F^+ et c' dans k , on aura alors :

$$\nu' A_{\bar{K}} = \mathfrak{G}' A_{\bar{K}} \quad \text{et} \quad \nu^{\sigma+1} A_k = \mathfrak{G}^2, \quad \nu'^{\sigma+1} A_k = \mathfrak{G}'^2$$

idéaux de k dans le groupe des idéaux de k' . On notera P_k le sous-groupe de $\mathcal{H}_k$ engendré par les classes d'idéaux principaux au sens ordinaire. On appellera $E_{k'}$ et E_k les groupes d'unités de k' et k . La notation $\dim_{\mathbf{Z}}$ conserve le même sens.

Posons

$$\begin{aligned} n'_1 &= \dim_{\mathbf{Z}} E_{k'} - \dim_{\mathbf{Z}} E_k, \\ n'_2 &= \dim_2 E_k^+ \cap Nk' / E_k^2 N E_{k'}, \\ n'_3 &= \dim_2 \mathcal{H}_k^{(2)} / \text{Ker } j' P_k. \end{aligned}$$

En utilisant des méthodes analogues à celles qui sont développées dans les paragraphes précédents, on obtient :

PROPOSITION 4a. — *Pour toute puissance de 2, notée m et comprise entre 4 et m_0 , on a :*

$$\dim_m \mathcal{H}_k - \dim_m \mathcal{H}_{k'} / j'(\mathcal{H}_k) \leq n'_1 + n'_2 + n'_3 + 1.$$

Si l'on pose

$$n''_1 = \dim_{\mathbf{Z}} E_k \quad \text{et} \quad n''_2 = \dim_2 \mathcal{H}_k^{(2)} / P_k,$$

on obtient :

PROPOSITION 4b. — *Pour toute puissance de 2, notée m et comprise entre 4 et m_0 , on a :*

$$\dim_m \mathcal{H}_{k'} / j'(\mathcal{H}_k) - \dim_m \mathcal{H}_k \leq n''_1 + n''_2.$$

5. Cas particuliers.

Revenons au théorème énoncé au paragraphe 3. Si le corps de base k est 2-principal, la constante n_3 est nulle. Si de plus, on suppose que k est 2-principal au sens restreint et totalement réel, alors $E_k^+ = E_k^2$ et $n_2 = 0$. Il s'en suit :

PROPOSITION 5. — *Supposons que le corps de base k soit 2-principal (au sens restreint) et totalement réel. Pour toute puissance de 2, notée m , supérieure à 4 et telle que k contienne $\mathbf{Q}_0^{(m)}$, les différences des m -rangs des groupes $\mathcal{H}_K$ et $\mathcal{H}_{\bar{K}}$ sont majorées par :*

$$\dim_m \mathcal{H}_K - \dim_m \mathcal{H}_{\bar{K}} \leq \dim_{\mathbf{Z}} E_{\bar{K}} - \dim_{\mathbf{Z}} E_k.$$

d'où :

$$\mathfrak{C}\mathfrak{C}'^{-1} = cc'^{-1}A_k \quad \text{et} \quad \text{Cl}(\mathfrak{C}\mathfrak{C}'^{-1})$$

appartient à P_k . Nous avons donc défini une application de $k^2\text{NF}^+$ dans $\text{Ker } \bar{j}/P_k \cap \text{Ker } \bar{j}$. C'est un homomorphisme surjectif et $k^2\text{NF}'^+$ est inclus dans son noyau. En factorisant, on obtient la dernière suite exacte.

Nous en déduisons :

$$\begin{aligned} \dim_2 C \cap N\bar{K}^+/k^2\text{NF}^+ &\leq \dim_2 C \cap N\bar{K}^+/C' \cap N\bar{K}^+ \\ &+ \dim_2 C' \cap N\bar{K}^+/k^2\text{NF}'^+ - \dim_2 k^2\text{NF}^+/k^2\text{NF}'^+ \\ &\leq \dim_2 \mathcal{H}_k^{(2)}/P_k + n_2 - \dim_2 \text{Ker } \bar{j}P_k/P_k = n_2 + n_3. \end{aligned}$$

On déduit alors des propositions 3a, b et c l'inégalité : $\dim_2 B^{**}/\pm B^{*2} \leq n_1 + n_2 + n_3$. Compte-tenu du corollaire énoncé à la fin du paragraphe 2, nous avons démontré :

THÉORÈME. — Soient n_1, n_2, n_3 les trois constantes définies par :

$$\begin{aligned} n_1 &= \dim_{\mathbf{Z}} E_{\bar{K}} - \dim_{\mathbf{Z}} E_k, \\ n_2 &= \dim_2 (E_k^+ \cap N\bar{K})/E_k^2 N E_{\bar{K}}^{\pm}, \\ n_3 &= \dim_2 \mathcal{H}_k^{(2)}/\text{Ker } \bar{j}P_k. \end{aligned}$$

Pour toute puissance de 2, notée m , supérieure à 4 et telle que $\mathbf{Q}_0^{(m)}$ soit inclus dans le corps de base k , les différences des m -rangs des groupes $\mathcal{D} = \mathcal{H}_k/j(\mathcal{H}_k)$ et $\bar{\mathcal{D}} = \mathcal{H}_{\bar{K}}/\bar{j}(\mathcal{H}_k)$ sont majorées par :

$$\dim_m \mathcal{D} - \dim_m \bar{\mathcal{D}} \leq n_1 + n_2 + n_3.$$

4. Deux autres inégalités.

Nous désignerons encore par k un corps de nombres ne contenant pas $\sqrt{-1}$ et par m_0 le plus grand entier tel que $\mathbf{Q}_0^{(m_0)}$ soit inclus dans k . On posera $k' = k(\sqrt{-1})$ et on notera N au lieu de $N_{k'/k}$ la norme dans l'extension k'/k . On désignera par $\mathcal{H}_k$ et $\mathcal{H}_{k'}$ les 2-groupes des classes au sens restreint de k et k' et par j' l'application de $\mathcal{H}_k$ dans $\mathcal{H}_{k'}$ déduite de l'injection canonique du groupe des

1) *Résultat de Damey-Payan* [2]. Posons $k = \mathbf{Q}$.

Désignons par a un entier sans facteur carré positif. Pour $d = a$, on a :

$$n_1 = \dim_{\mathbf{Z}} E_{\mathbf{Q}(\sqrt{-a})} - \dim_{\mathbf{Z}} E_{\mathbf{Q}} = 0$$

et pour $d = -a$, on a :

$$n_1 = \dim_{\mathbf{Z}} E_{\mathbf{Q}(\sqrt{a})} - \dim_{\mathbf{Z}} E_{\mathbf{Q}} = 1.$$

On en déduit :

$$0 \leq \dim_4 \mathcal{H}_{\mathbf{Q}(\sqrt{-a})} - \dim_4 \mathcal{H}_{\mathbf{Q}(\sqrt{a})} \leq 1.$$

En affinant certains détails de la démonstration générale on peut montrer de plus :

Si la norme de l'unité fondamentale de $\mathbf{Q}(\sqrt{a})$ est égale à -1 et si $a \not\equiv 1 \pmod{8}$, alors la différence des 4-rangs des groupes des classes de $\mathbf{Q}(\sqrt{a})$ et $\mathbf{Q}(\sqrt{-a})$ est nulle.

Remarquons que si $a \equiv 1 \pmod{8}$, alors la différence en question peut prendre l'une ou l'autre des valeurs 0 ou 1; (par exemple : $a = 17$ et $a = 3 \cdot 161$).

On en déduit qu'il existe une infinité d'entiers a sans facteur carré tels que la différence des 4-rangs des groupes des classes de $\mathbf{Q}(\sqrt{a})$ et $\mathbf{Q}(\sqrt{-a})$ prenne la valeur 0. D'autre part, il existe également une infinité d'entiers a sans facteur carré tels que la différence en question ait pour valeur 1. En effet, lorsque p est premier congru à 1 modulo 8, $\mathbf{Q}(\sqrt{p})$ est 2-principal et le 2-groupe des classes de $\mathbf{Q}(\sqrt{-p})$ est cyclique d'ordre divisible par 4.

2) *Résultat de L. Bouvier* [1]. Posons $k = \mathbf{Q}(\sqrt{2})$. Désignons encore par a un entier sans facteur carré positif. Pour $d = a$ nous aurons : $n_1 = 0$ et pour $d = -a$: $n_1 = 2$. On en déduit les inégalités suivantes, qui améliorent [1] :

$$0 \leq \dim_m \mathcal{H}_{\mathbf{Q}(\sqrt{2}, \sqrt{-a})} - \dim_m \mathcal{H}_{\mathbf{Q}(\sqrt{2}, \sqrt{a})} \leq 2,$$

pour $m = 4$ et 8.

Chacune des différences peut donc prendre trois valeurs. Nous nous sommes demandés si les neuf cas existent réellement. Pour cela nous avons programmé le calcul des 4-rangs et 8-rangs des groupes des classes de $\mathbf{Q}(\sqrt{2}, \sqrt{a})$ et $\mathbf{Q}(\sqrt{2}, \sqrt{-a})$

à l'aide de la méthode de Gras [3]. Nous avons mis en évidence huit cas distincts. .

Le tableau suivant contient un exemple de chacun d'eux. On trouve sur la même ligne que a , les 4-rangs et les 8-rangs de $\mathbf{Q}(\sqrt{2}, \sqrt{a})$ et $\mathbf{Q}(\sqrt{2}, \sqrt{-a})$.

a	4-rangs	8-rangs	a	4-rangs	8-rangs
3	0 0	0 0	69	0 2	0 0
15	0 1	0 0	257	1 2	0 2
33	0 1	0 1	395	0 2	0 2
65	1 1	0 1	573	0 2	0 1

Pour a variant de 3 à 3 500, il n'existe pas d'exemple où la différence des 4-rangs soit nulle et la différence des 8-rangs égale à 2.

3) *Un exemple où la différence des 4-rangs de $\mathcal{D}$ et $\overline{\mathcal{D}}$ dépasse n_1 .*

La propriété de Damey-Payan présente une grande analogie avec la propriété de Scholtz [6]. De même que nous généralisons ici la première en essayant de remplacer $\mathbf{Q}$ par un corps de base plus général, de même nous avons essayé de généraliser celle de Scholtz. (En fait, on peut même le faire avec le « Spiegelungssatz ». Le problème ne présente d'ailleurs aucune difficulté. La démonstration de Leopoldt se transpose immédiatement. On pourra trouver les détails dans [5]). Le résultat obtenu est le suivant :

Désignons momentanément par :

k un corps de nombres ne contenant pas $\sqrt{-3}$,

d un élément de k tel que ni $\sqrt{d}$, ni $\sqrt{-3d}$ n'appartiennent à k ,

$K = k(\sqrt{d})$, $\overline{K} = k(\sqrt{-3d})$, $k' = k(\sqrt{-3})$,

$\mathcal{H}_K$, $\mathcal{H}_{\overline{K}}$, $\mathcal{H}_{k'}$, $\mathcal{H}_k$ les 3-groupes des classes de K , $\overline{K}$, k' et k ,

j , $\overline{j}$, j' les applications de $\mathcal{H}_k$ dans $\mathcal{H}_K$, $\mathcal{H}_{\overline{K}}$, $\mathcal{H}_{k'}$ déduites

des injections canoniques du groupe des idéaux de k dans les groupes d'idéaux de K , $\bar{K}$ et k' .

Les notations $E_{\bar{K}}$, $E_{k'}$, E_k , $\dim_{\mathbf{Z}}$ ont toujours la même signification. Nous démontrons dans [5] les inégalités :

$$(1) \dim_m \mathcal{H}_{\bar{K}}/j(\mathcal{H}_k) - \dim_m \mathcal{H}_{\bar{K}}/\bar{j}(\mathcal{H}_k) \leq \dim_{\mathbf{Z}} E_{\bar{K}} - \dim_m E_k$$

$$(2) \dim_m \mathcal{H}_k - \dim_m \mathcal{H}_{k,|j'}(\mathcal{H}_k) \leq \dim_{\mathbf{Z}} E_{k'} - \dim_{\mathbf{Z}} E_k + 1,$$

$$(3) \dim_m \mathcal{H}_{k'}/j'(\mathcal{H}_k) - \dim_m \mathcal{H}_k \leq \dim_{\mathbf{Z}} E_k,$$

pour toute puissance de 3 notée m et, telle que $\mathbf{Q}_0^{(m)}$ soit inclus dans k .

Le théorème du paragraphe 3 est donc l'analogue de l'inégalité (1). Les deux autres inégalités : (2) et (3) correspondent aux propositions 4a et b. Il est curieux de constater, que les bornes obtenues ne sont pas les mêmes (alors que dans les propriétés de Damey-Payan et Scholtz, elles coïncidaient). C'est la raison pour laquelle nous avons cherché un exemple où la différence des 4-rangs de $\mathcal{D}$ et $\bar{\mathcal{D}}$ soit strictement supérieure à $n_1 = \dim_{\mathbf{Z}} E_{\bar{K}} - \dim_{\mathbf{Z}} E_k$.

Posons $k = \mathbf{Q}(\sqrt{-2})$. Ce corps est principal. Nous aurons donc $n_3 = 0$, $\mathcal{D} = \mathcal{H}_{\bar{K}}$ et $\bar{\mathcal{D}} = \mathcal{H}_{\bar{K}}$. Prenons pour d un entier sans facteur carré. La constante n_1 vaut alors 1 et n_2 vaut 0 ou 1 suivant les cas :

- Si -1 est norme d'une unité dans $\bar{K}/k$, alors $n_2 = 0$.
- Si -1 est norme dans $\bar{K}/k$ sans être norme d'unité, alors $n_2 = 1$.
- Si -1 n'est pas norme dans $\bar{K}/k$, alors $n_2 = 0$.

Nous avons programmé le calcul de la différence

$$\dim_4 \mathcal{H}_{\bar{K}} - \dim_4 \mathcal{H}_{\bar{K}},$$

à l'aide de la méthode de Gras [3].

Pour $d = 1\,679$ cette différence vaut 2. Signalons que ce fait ne se produit qu'une seule fois, lorsque d varie de 3 à 2\,500.

BIBLIOGRAPHIE

- [1] L. BOUVIER, Sur le 2-groupe des classes de certains corps biquadratiques, 3^e cycle, Grenoble.
- [2] P. DAMEY et J. J. PAYAN, Existence et construction des extensions

RELATIONS ENTRE LES 2 GROUPES DES CLASSES D'IDÉAUX 59

- galoisiennes et non abéliennes de degré 8 d'un corps de caractéristique différente de 2, *Jour. für die reine und angew. Math.*, 244 (1970).
- [3] G. GRAS, Sur les l -classes d'idéaux dans les extensions cycliques relatives de degré premier l , *Ann. de l'Institut Fourier*, 23 (1973), 1-48.
 - [4] H. W. LEOPOLDT, Zur Struktur der l -Klassengruppe galoischer Zahlkörper, *Journ. für die reine und angew. Math.*, 199 (1958), 165-175.
 - [5] B. ORLAT, Spiegelungssatz, Publications Mathématiques de la Faculté des Sciences de Besançon (1975).
 - [6] A. SCHOLTZ, Über die Beziehung der Klassenzahlen quadratischer Körper zueinander, *Jour. für die reine und angew. Math.*, 166 (1931), 201-203.

Manuscrit reçu le 13 avril 1976

Proposé par J. Martinet.

Bernard ORLAT,

Faculté des Sciences

Route de Gray

25030 Besançon Cedex.

2,4 ET 8-RANG DU GROUPE DES CLASSES

D'IDEAUX DE $\mathbb{Q}(\sqrt{2}, \sqrt{d})$; $|d| \leq 1000$

Bernard Oriat

Soit a un entier sans facteur carré, compris entre 3 et 1000, impair.

La table 1 donne les 2-rang, 4-rang et 8-rang du groupe des classes d'idéaux de $\mathbb{Q}(\sqrt{2}, \sqrt{-a})$ et l'exposant de 2 dans la décomposition en facteurs premiers du nombre de classes de ce corps. Les valeurs de a , telles que le 4-rang du groupe des classes d'idéaux de $\mathbb{Q}(\sqrt{2}, \sqrt{-a})$ soit nul, ont été omises.

La table 2 donne les 2-rang, 4-rang et 8-rang du groupe des classes au sens restreint de $\mathbb{Q}(\sqrt{2}, \sqrt{a})$. De même qu'à la table précédente, les valeurs de a telles que le 4-rang soit nul, ont été omises.

La méthode employée a été développée par G. Gras dans [1]. Précisons que si t est le nombre d'idéaux premiers de $\mathbb{Q}(\sqrt{2})$ ramifiés dans $\mathbb{Q}(\sqrt{2}, \sqrt{d})$, le 2-rang du groupe des classes (au sens restreint) de ce corps est $t-1$; ([1] Th IV). D'autre part, il existe des formules liant le nombre de classes d'un corps biquadratique bicyclique aux nombres de classes de ses trois sous-corps quadratiques [2]. En particulier, le nombre de classes de $\mathbb{Q}(\sqrt{2}, \sqrt{-a})$ est égal au demi-produit des nombres de classes des corps $\mathbb{Q}(\sqrt{-a})$

et $\mathbb{Q}(\sqrt{-2a})$. C'est ainsi qu'a été calculé l'exposant de 2 dans la décomposition en facteurs premiers du nombre de classes de $\mathbb{Q}(\sqrt{2}, \sqrt{-a})$.

Signalons enfin que les 4-rangs et 8-rangs des groupes des classes d'idéaux de $\mathbb{Q}(\sqrt{2}, \sqrt{a})$ et $\mathbb{Q}(\sqrt{2}, \sqrt{-a})$ sont liés par les relations:

$$0 \leq \dim_m \mathcal{H}_{\mathbb{Q}(\sqrt{2}, \sqrt{-a})} - \dim_m \mathcal{H}_{\mathbb{Q}(\sqrt{2}, \sqrt{a})} \leq 2, \quad (m=4 \text{ ou } 8).$$

On trouvera une démonstration de ces inégalités dans [3].

[1] Gras (G.), Sur les ℓ -classes d'idéaux dans les extensions cycliques relatives de degré premier ℓ , Ann. Inst. Fourier, 23 (1973).

[2] Hasse (H.), Über die Klassenzahl abelscher Zahlkörpern, Berlin, (1952).

[3] Oriat (B.), Relations entre les 2-groupes des classes d'idéaux des extensions quadratiques $k(\sqrt{d})$ et $k(\sqrt{-d})$, Ann. Inst. Fourier, 27 (1977).

Table 1 (Corps imaginaires)

15	1 1 0	2	201	2 1 1	5	335	1 1 0	2
17	2 1 0	3	203	2 1 1	5	337	2 2 1	5
31	1 1 0	2	205	3 1 1	6	345	4 1 1	6
33	2 1 1	4	209	2 1 1	4	353	2 2 1	6
39	1 1 1	3	213	3 2 0	5	355	2 1 1	6
41	2 1 1	4	215	1 1 0	2	367	1 1 0	2
47	1 1 0	2	217	4 1 0	5	371	2 1 1	5
55	1 1 1	3	219	2 2 0	4	377	2 1 1	5
57	2 1 1	4	221	3 1 1	6	383	1 1 0	2
65	2 1 1	4	223	1 1 1	4	385	4 1 1	7
69	3 2 0	5	231	3 1 0	4	393	2 1 1	5
73	2 1 1	5	233	2 1 1	4	395	2 2 2	6
77	3 2 0	5	239	1 1 0	2	399	3 2 1	7
79	1 1 0	2	241	2 1 0	3	401	2 1 0	3
87	1 1 0	2	247	1 1 0	2	407	1 1 1	5
89	2 1 1	4	249	2 1 1	4	409	2 1 1	5
95	1 1 1	4	255	3 1 1	5	415	1 1 0	2
97	2 1 0	3	257	2 2 2	7	417	2 1 1	5
105	4 1 0	5	259	2 1 1	5	429	3 2 2	7
111	1 1 1	4	265	2 1 1	4	431	1 1 0	2
113	2 2 1	5	271	1 1 0	2	433	2 1 0	3
127	1 1 1	3	273	4 1 0	5	435	2 2 1	5
129	2 1 1	4	281	2 1 1	4	445	3 2 0	5
137	2 1 1	4	285	3 2 2	7	447	1 1 0	2
141	3 2 0	5	287	3 1 0	4	449	2 1 0	3
143	1 1 0	2	291	2 1 1	5	455	3 1 1	5
145	2 1 1	4	295	1 1 1	4	457	2 1 1	4
155	2 2 0	4	299	2 1 1	5	463	1 1 0	2
159	1 1 0	2	301	3 2 0	5	465	4 1 1	6
161	4 1 1	6	303	1 1 0	2	469	3 2 2	7
165	3 2 0	5	305	2 1 1	5	471	1 1 1	5
177	2 1 1	5	313	2 1 1	4	473	2 1 1	5
183	1 1 1	4	319	1 1 0	2	479	1 1 1	3
185	2 1 1	5	321	2 1 1	5	481	2 1 1	5
191	1 1 0	2	323	2 1 1	5	489	2 1 1	4
193	2 1 0	3	327	1 1 1	3	497	4 1 1	6
195	2 2 1	5	329	4 1 0	5	501	3 2 2	7

505 2 1 1 4
511 3 1 1 5
519 1 1 0 2
521 2 1 1 6
527 3 1 0 4
535 1 1 0 2
537 2 1 1 6
543 1 1 1 3
545 2 1 1 6
551 1 1 0 2
553 4 1 1 6
555 2 2 1 5
559 1 1 1 5
561 4 2 1 7
569 2 1 1 6
573 3 2 1 8
577 2 2 1 5
579 2 1 1 5
583 1 1 1 4
589 3 2 2 7
591 1 1 0 2
593 2 2 1 5
601 2 1 1 4
607 1 1 0 2
609 4 1 1 6
615 3 1 0 4
617 2 1 1 4
623 3 1 0 4
627 2 2 0 4
633 2 1 1 6
641 2 1 0 3
645 3 2 2 7
649 2 1 1 6
651 4 2 0 6
655 1 1 1 3
663 3 1 1 6
665 4 1 0 5
667 2 1 1 6
671 1 1 0 2

673 2 1 0 3
681 2 1 1 4
687 1 1 1 3
689 2 1 1 4
695 1 1 1 4
697 4 1 1 6
703 1 1 0 2
705 4 1 1 7
713 4 1 1 7
715 2 2 1 6
717 3 2 1 8
719 1 1 1 3
721 4 1 1 6
723 2 1 1 6
731 2 1 1 5
737 2 1 1 5
741 3 2 0 5
745 2 1 1 5
749 3 2 1 8
751 1 1 0 2
753 2 1 1 4
755 2 1 1 5
759 3 1 1 5
761 2 1 1 4
763 2 1 1 5
767 1 1 0 2
769 2 1 0 3
777 4 1 1 6
785 2 1 1 5
789 3 2 1 8
791 3 1 1 8
793 2 1 1 4
795 2 2 2 6
799 3 2 1 8
805 5 1 1 8
807 1 1 0 2
809 2 1 1 6
815 1 1 0 2
817 2 1 1 7

831 1 1 1 3
849 2 1 1 5
857 2 1 1 6
863 1 1 0 2
865 2 1 1 5
869 3 2 1 8
871 1 1 0 2
879 1 1 0 2
881 2 2 1 5
885 3 2 0 5
889 4 1 1 6
895 1 1 1 5
897 4 2 1 8
901 3 1 1 7
903 3 1 1 6
905 2 1 1 4
911 1 1 1 3
913 2 1 1 4
915 2 2 1 5
921 2 1 1 5
929 2 1 0 3
933 3 2 1 8
935 3 1 1 5
937 2 1 1 4
939 2 1 1 5
943 3 2 2 9
951 1 1 0 2
953 2 1 1 6
955 2 2 0 4
957 3 2 2 7
959 3 1 1 5
969 4 1 1 7
977 2 1 0 3
979 2 2 1 7
985 2 1 1 4
987 4 1 1 7
991 1 1 0 2
993 2 1 1 5
995 2 1 1 5

Table 2 (Corps réels)

65	1 1 0	435	3 1 1	745	1 1 0
113	1 1 0	445	2 1 0	777	3 1 1
145	1 1 1	455	4 1 0	785	1 1 0
165	2 1 0	465	3 1 0	791	4 1 0
185	1 1 0	481	1 1 0	793	1 1 1
195	3 1 0	497	3 1 0	795	3 1 1
205	2 1 0	505	1 1 1	799	4 1 1
219	3 2 0	545	1 1 0	865	1 1 0
221	2 1 0	555	3 1 0	881	1 1 0
255	4 1 0	561	3 1 0	885	2 1 0
257	1 1 0	577	1 1 0	897	3 1 0
265	1 1 0	579	3 1 0	901	2 1 0
285	2 1 0	593	1 1 0	905	1 1 1
291	3 1 0	609	3 1 0	915	3 1 0
305	1 1 0	627	3 2 0	935	4 1 0
323	3 1 1	645	2 1 1	939	3 1 0
337	1 1 0	689	1 1 1	943	4 1 0
353	1 1 0	715	3 1 0	957	2 1 1
377	1 1 0	723	3 1 1	959	4 1 0
399	4 1 0	731	3 1 0	979	3 2 0
429	2 1 0	741	2 1 0	985	1 1 0

Sur la divisibilité par 8 et 16 des nombres de classes d'idéaux des corps quadratiques $Q(\sqrt{2p})$ et $Q(\sqrt{-2p})$.

Par Bernard ORIAT

(Reçu le 6 juil., 1976)

Introduction.

Soit p un nombre premier congru à 1 modulo 8. Notons $h(d)$ le nombre de classes d'idéaux au sens restreint du corps quadratique $Q(\sqrt{d})$. Nous démontrons ci-après les implications :

A : Si $h(2p) \equiv 0 \pmod{8}$, alors $h(-2p) \equiv 0 \pmod{8}$;

B : Si $h(2p) \equiv 0 \pmod{16}$, alors $h(-2p) \equiv 0 \pmod{16}$.

L'implication A a été énoncée et démontrée à l'aide de formes quadratiques par P. Kaplan ; [3]. Celui-ci a montré d'ailleurs le résultat plus précis :

$h(2p) \equiv 0 \pmod{8}$ si et seulement si $h(-p) \equiv 0 \pmod{8}$ et $h(-2p) \equiv 0 \pmod{8}$.

Le paragraphe I est consacré à la démonstration de l'implication A. Elle est obtenue comme conséquence des résultats exposés dans [6]. Le paragraphe II contient la démonstration de B. Celle-ci n'est pas conséquence de [6], mais la plupart des principes appliqués dans [6] (et en particulier la "Spiegelungsrelation" de Leopoldt [5]) seront encore utilisés. On donne dans le paragraphe III quelques contre-exemples à des implications du même type que celles énoncées ci-dessus.

RAPPELS. Si p est un nombre premier (impair) le 2-groupe des classes d'idéaux (au sens restreint) de $Q(\sqrt{2p})$ est cyclique. Si p n'est pas congru à 1 modulo 8, il est exactement d'ordre 2. Si p est congru à 1 modulo 8, il est d'ordre au moins égal à 4.

De la même façon, le 2-groupe des classes d'idéaux de $Q(\sqrt{-2p})$ est cyclique. Si p n'est pas congru ± 1 modulo 8, il est exactement d'ordre 2. Si p est congru à ± 1 modulo 8, il est d'ordre au moins égal à 4.

NOTATIONS. Dans toute la suite, on supposera que p est premier congru à 1 modulo 8. Il ne sera question que de classes d'idéaux au sens restreint.

Le 2-groupe des classes d'idéaux du corps de nombres L sera noté $\mathfrak{H}_L$.

I. Démonstration de l'implication A.

Rappelons que nous avons démontré dans [6] le résultat suivant :

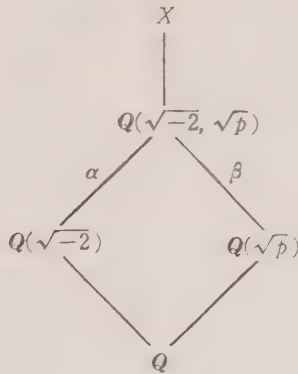
PROPOSITION I. Soit k un corps de nombres 2-principal et totalement réel. Soit d un élément de k . On suppose qu'aucune des quantités $\sqrt{d}$, $\sqrt{-d}$, $\sqrt{-1}$ n'appartient à k . Soient $K=k(\sqrt{d})$ et $\bar{K}=k(\sqrt{-d})$. Soient $E_{\bar{K}}$ et E_k les groupes d'unités de $\bar{K}$ et k . Soit m une puissance de 2, supérieure à 4 et telle que k contienne $\mathbb{Q}_0^{(m)}$, sous-corps réel maximal du $m^{\text{ème}}$ corps cyclotomique. Alors la différence des m -rangs des groupes des classes $\mathfrak{H}_K$ et $\mathfrak{H}_{\bar{K}}$ vérifie l'inégalité :

$$\dim_m \mathfrak{H}_K - \dim_m \mathfrak{H}_{\bar{K}} \leq \dim_Z E_{\bar{K}} - \dim_Z E_k.$$

Si nous appliquons ce résultat à $k=\mathbb{Q}(\sqrt{p})$ et $d=2$, nous obtenons :

$$\dim_4 \mathfrak{H}_{\mathbb{Q}(\sqrt{-2}, \sqrt{p})} \leq \dim_4 \mathfrak{H}_{\mathbb{Q}(\sqrt{-2}, \sqrt{p})}.$$

Supposons $h(2p) \equiv 0 \pmod{8}$. Le corps quadratique $\mathbb{Q}(\sqrt{2p})$ possède une extension non ramifiée cyclique de degré 8 et son corps des genres est $\mathbb{Q}(\sqrt{-2}, \sqrt{p})$. Il s'en suit : $\dim_4 \mathfrak{H}_{\mathbb{Q}(\sqrt{-2}, \sqrt{p})} \neq 0$. D'après l'inégalité ci-dessus, on aura donc : $\dim_4 \mathfrak{H}_{\mathbb{Q}(\sqrt{-2}, \sqrt{p})} \neq 0$. Soit X la 2-extension abélienne non ramifiée maximale de $\mathbb{Q}(\sqrt{-2}, \sqrt{p})$. Soit α (resp. β) l'automorphisme de $\mathbb{Q}(\sqrt{-2}, \sqrt{p})/\mathbb{Q}(\sqrt{-2})$ (resp. $\mathbb{Q}(\sqrt{-2}, \sqrt{p})/\mathbb{Q}(\sqrt{p})$) différent de 1 et soit a (resp. b) un prolongement de α (resp. β) à X . Puisque $\mathbb{Q}(\sqrt{-2})$ est principal, on a pour tout x de



$\text{Gal}(X/\mathbb{Q}(\sqrt{-2}, \sqrt{p}))$: $a^{-1}xa = x^{-1}$. De même $b^{-1}xb = x^{-1}$. D'où $abx = xab$ et l'extension $X/\mathbb{Q}(\sqrt{-2p})$ est abélienne. Il s'en suit que X est aussi la 2-extension abélienne non ramifiée maximale de $\mathbb{Q}(\sqrt{-2p})$. Nous aurons donc $h(-2p) \equiv 0 \pmod{8}$. (On aurait pu aussi employer à la place de ce dernier argument, la formule

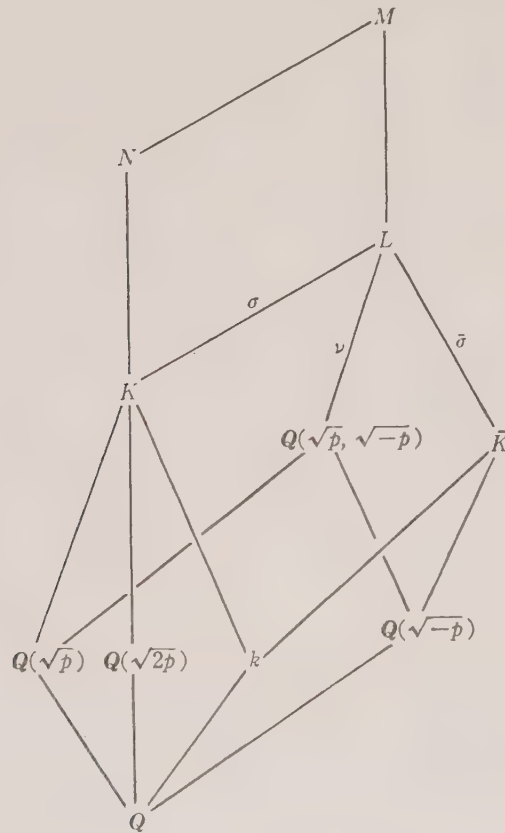
analytique liant le nombre de classes de $Q(\sqrt{-2}, \sqrt{p})$ aux nombres de classes de $Q(\sqrt{-2}, \sqrt{p})$ aux nombres de classes de ses sous-corps quadratiques; [2] § 26; ou bien, la formule des classes ambiges ([1] Théorème IV 1), appliquée à $Q(\sqrt{-2}, \sqrt{p})/Q(\sqrt{-2p})$.

II. Démonstration de l'implication B.

Cette démonstration sera réalisée en deux étapes. Démontrons d'abord la

PROPOSITION II a: Si $h(2p) \equiv 0 \pmod{16}$, alors il existe une classe d'idéaux de $Q(\sqrt{2}, \sqrt{-p})$ d'ordre 8 exactement, dont le carré est une classe ambige dans l'extension $Q(\sqrt{2}, \sqrt{-p})/Q(\sqrt{-2p})$.

DÉMONSTRATION. Posons $k=Q(\sqrt{2})$, $K=Q(\sqrt{2}, \sqrt{p})$, $\bar{K}=Q(\sqrt{2}, \sqrt{-p})$. Supposons donc $h(2p) \equiv 0 \pmod{16}$. Le corps quadratique $Q(\sqrt{2p})$ possède une ex-



tension non ramifiée cyclique de degré 16 que l'on notera N . Comme le corps des genres de $Q(\sqrt{2p})$ est K , on en déduit que K est inclus dans N et que l'extension N/K est non ramifiée cyclique de degré 8. (On peut alors déduire de la proposition I rappelée ci-dessus, l'existence d'un élément d'ordre 8 dans $\mathfrak{H}_{\bar{K}}$. Mais ce résultat ne suffit pas pour conclure).

Soit $L=Q(\sqrt{2}, \sqrt{p}, \sqrt{-1})$ et soit σ (resp. $\bar{\sigma}; \nu$) l'élément de $\text{Gal}(L/Q)$ invariant K (resp. $\bar{K}; Q(\sqrt{p}, \sqrt{-p})$). Posons $M=NL$. L'extension M/L est une extension de Kummer de degré 8 exactement et on note W son radical, c'est-à-dire :

$$W = \{w; w \in M, w^8 \in L^*\}.$$

Si τ appartient à $\text{Gal}(L/Q)$, soit t un prolongement de τ à M . Le groupe W/L^* est muni de la structure de $\text{Gal}(L/Q)$ -module définie par $(wL^*)^\tau = w^t L^*$. Précisons cette structure :

Soit s (resp. $\bar{s}; \nu$) un prolongement de σ (resp. $\bar{\sigma}, \nu$) à M et soit x un élément de $\text{Gal}(M/L)$. On a alors : $s^{-1}xs = x$; $\bar{s}^{-1}x\bar{s} = x^{-1}$ et $\nu^{-1}x\nu = x^{-1}$. D'autre part, si ζ désigne une racine 8^{ème} de 1, nous avons : $\zeta^\sigma = \zeta^{-1}$; $\zeta^{\bar{\sigma}} = \zeta^{-1}$ et $\zeta^\nu = \zeta^5$. On déduit alors de la "Spiegelungsrelation" ([5] ou [7]) : $(wL^*)^\sigma = (wL^*)^{-1}$; $(wL^*)^{\bar{\sigma}} = wL^*$ et $(wL^*)^\nu = (wL^*)^5$.

Nous allons montrer que les deux premières égalités peuvent être précisées : L'extension N/K est décomposée sur k . Il en est de même de M/L sur $\bar{K}$. Si $\bar{s}$ est un prolongement d'ordre 2 de $\bar{\sigma}$ à M , on désigne par W' l'ensemble des éléments de W invariants par $\bar{s}$.

Considérons l'injection canonique de W' dans W . Elle induit un homomorphisme injectif de $W'/\bar{K}^*$ dans W/L^* . Montrons qu'il s'agit d'un isomorphisme : Si w appartient à W , $w^{\bar{s}-1}$ appartient à L^* et vérifie $(w^{\bar{s}-1})^{\bar{\sigma}+1} = 1$. Il existe donc un élément α de L^* tel que $\alpha^{\bar{\sigma}-1} = w^{\bar{s}-1}$. On en déduit que $w\alpha^{-1}$ appartient à W' et que $W'/\bar{K}^*$ est isomorphe à W/L^* .

Montrons aussi que si w appartient à W' , alors $w^{8(\sigma+1)}$ appartient à k^8 . Nous pouvons supposer que s a pour ordre 2. Nous aurons alors $s^2 = 1$ et $s\bar{s} = \bar{s}s$. Comme w^{s+1} appartient à L^* , on en déduit que w^{s+1} appartient à k , c'est-à-dire que $w^{8(\sigma+1)}$ appartient à k^8 . (Ces résultats étaient déjà énoncés dans [6]; Proposition II b).

Nous pouvons construire maintenant un homomorphisme θ de $W'/\bar{K}^*$ dans $\mathfrak{H}_{\bar{K}}$ de la façon suivante : Si w appartient à W' , w^8 appartient à $\bar{K}$ et engendre dans L un idéal qui est une puissance 8^{ème} d'un idéal de L . Cet idéal est invariant par $\bar{\sigma}$ et l'extension $L/\bar{K}$ est non ramifiée. Cet idéal est donc l'étendu d'un idéal $\mathfrak{a}$ de $\bar{K}$ et nous avons : ($A_{\bar{K}}$ étant l'anneau des entiers de $\bar{K}$)

$$w^8 A_{\bar{K}} = \mathfrak{a}^8.$$

En associant à $w\bar{K}^*$ la classe de $\mathfrak{a}$, on définit un homomorphisme θ de $W'/\bar{K}^*$ dans $\mathfrak{H}_{\bar{K}}$.

Montrons que cet homomorphisme θ est injectif. Supposons que $\theta(w\bar{K}^*) = cl(\mathfrak{a})$ soit d'ordre 4 au plus. Alors il existe b dans $\bar{K}$ tel que $w^8 A_{\bar{K}} = b^2 A_{\bar{K}}$, avec $b A_{\bar{K}} = \mathfrak{a}^4$. Il existe une unité ε de $\bar{K}$ telle que $w^8 = b^2 \varepsilon$. Or le groupe des unités de $\bar{K}$ coïncide avec le groupe des unités de k ([2] Satz 25) et d'autre part, $b^{\sigma+1} A_{\bar{K}}$ est la puissance 4^{ème} d'un idéal de k . On a donc $b^{\sigma+1} = c^4 \varepsilon'$, avec c dans k et ε' unité de k . Cette unité est totalement positive. C'est donc un carré dans k et $b^{\sigma+1}$ est un carré dans k . De la relation $w^{8(\sigma+1)} = b^{2(\sigma+1)} \varepsilon^{\sigma+1} = b^{2(\sigma+1)} \varepsilon^2$ on déduit que ε^2 appartient à k^4 , c'est-à-dire que ε appartient à L^2 et w^4 appartient à $\bar{K}$. L'élément $w\bar{K}^*$ est donc d'ordre 4 au plus. Comme $W'/\bar{K}^*$ est cyclique d'ordre 8, nous avons montré que θ est injectif.

Utilisons maintenant l'égalité $(wL^*)^\nu = (wL^*)^3$. Si w appartient à W' , $w^{8(\nu-8)}$ appartient donc à $L^8 \cap \bar{K}$. On en déduit que $w^{8(\nu+1)}$ appartient à $L^4 \cap \bar{K}$. Un calcul élémentaire prouve que cette intersection est égale à $\bar{K}^4 \cup -\bar{K}^4$. Nous avons donc $w^{8(\nu+1)} = \pm b^4$ avec b dans $\bar{K}$. L'image de w par θ est définie par :

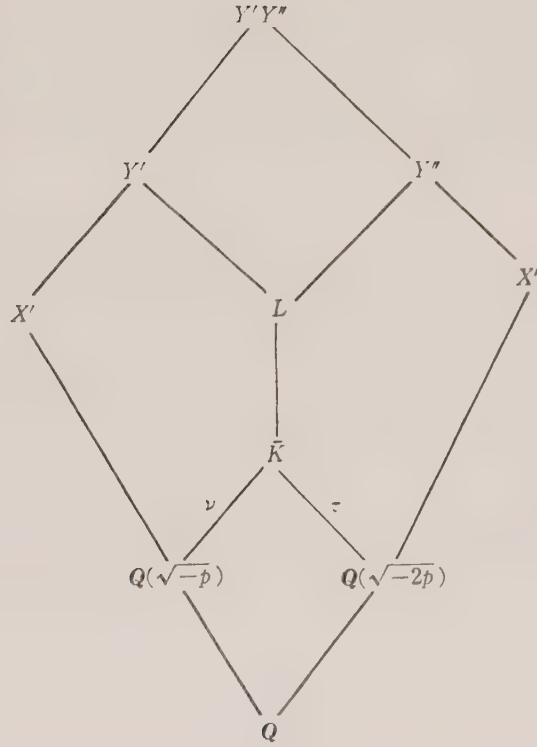
$$w^8 A_{\bar{K}} = \mathfrak{a}^8$$

et nous aurons donc $\mathfrak{a}^{2(\nu+1)} = b A_{\bar{K}}$. Ceci montre que $cl(\mathfrak{a})^{2(\nu+1)}$ est principale ; c'est-à-dire que $cl(\mathfrak{a})^2$ est ambige dans $\bar{K}/Q(\sqrt{-2p})$.

PROPOSITION II b. Si $Q(\sqrt{2}, \sqrt{-p})$ possède une classe d'idéaux d'ordre 8 exactement dont le carré est ambige dans $Q(\sqrt{2}, \sqrt{-p})/Q(\sqrt{-2p})$ et si $h(-p) \equiv 0 \pmod{8}$, alors $h(-2p) \equiv 0 \pmod{16}$.

DÉMONSTRATION. Notons encore $\bar{K}$ le corps $Q(\sqrt{2}, \sqrt{-p})$. Désignons par X' (resp. X'') la 2-extension abélienne maximale non ramifiée de $Q(\sqrt{-p})$ (resp. $Q(\sqrt{-2p})$). On posera $Y' = X'\bar{K}$, $Y'' = X''\bar{K}$, $G' = \text{Gal}(Y'/\bar{K})$ et $G'' = \text{Gal}(Y''/\bar{K})$. Les extensions $\bar{K}/Q(\sqrt{-p})$ et $\bar{K}/Q(\sqrt{-2p})$ sont ramifiées. Les groupes G' et G'' sont donc isomorphes aux 2-groupes des classes d'idéaux de $Q(\sqrt{-p})$ et $Q(\sqrt{-2p})$. Nous désignerons par ν et τ les automorphismes de $\bar{K}$ invariants par $Q(\sqrt{-p})$ et $Q(\sqrt{-2p})$.

Désignons encore par L le corps $Q(\sqrt{2}, \sqrt{-1}, \sqrt{p})$. Montrons que $L = Y' \cap Y''$. L'inclusion $L \subset Y' \cap Y''$ provient de ce que $Q(\sqrt{-1}, \sqrt{p})$ (resp. $Q(\sqrt{-2}, \sqrt{p})$) est le corps des genres de $Q(\sqrt{-p})$ (resp. $Q(\sqrt{-2p})$). Réciproquement, désignons par ν un prolongement de ν à $Y' \cap Y''$. Si x est un élément de $\text{Gal}(Y' \cap Y''/\bar{K})$, on aura : $\nu^{-1}x\nu = x$. D'autre part, en vertu de l'isomorphisme de réciprocité liant $\mathfrak{H}_{Q(\sqrt{-2p})}$ et $\text{Gal}(X''/Q(\sqrt{-2p}))$, on aura aussi $\nu^{-1}x\nu = x^{-1}$. Il s'en suit que $\text{Gal}(Y' \cap Y''/\bar{K})$ est d'exposant 2. Comme G' est cyclique, on a donc $[Y' \cap Y'' : \bar{K}] = 2$ ce qui démontre l'égalité $L = Y' \cap Y''$.



Le degré $[Y'Y'' : \bar{K}]$ est égal au demi-produit des 2-nombres de classes de $Q(\sqrt{-p})$ et $Q(\sqrt{-2p})$. Or d'après la formule analytique de [2] §26, ce nombre est égal au 2-nombre de classes de $\bar{K}$. La 2-extension abélienne non ramifiée maximale de $\bar{K}$ est donc $Y'Y''$. D'après l'isomorphisme de réciprocité, $\text{Gal}(Y'Y''/\bar{K})$ est isomorphe à $\mathfrak{H}_{\bar{K}}$.

D'autre part le groupe de Galois $\text{Gal}(Y'Y''/\bar{K})$ s'identifie canoniquement au sous-groupe $G' \overset{\circ}{\times} G''$ de $G' \times G''$ formé des couples (x', x'') tels que les restrictions de x' et x'' à L soient égales. Soit t un prolongement de τ à $Y'Y''$. Notons encore t les restrictions de t à Y' et Y'' . Nous avons :

$$t^{-1}(x', x'')t = (t^{-1}x't, t^{-1}x''t) = (x'^{-1}, x'').$$

Un élément (x', x'') de $G' \overset{\circ}{\times} G''$ correspond donc à une classe d'idéaux de $\bar{K}$, ambige dans $\bar{K}/Q(\sqrt{-2p})$, si et seulement si $x'^2=1$.

Supposons donc que $\mathfrak{H}_{\bar{K}}$ possède un élément d'ordre 8, dont le carré est ambige dans $\bar{K}/Q(\sqrt{-2p})$. Il existe donc dans $G' \overset{\circ}{\times} G''$ un élément (x', x'') d'ordre 8 tel que $x'^4=1$. L'ordre de x'' est exactement 8. Si $h(-p) \equiv 0 \pmod{8}$, le

groupe G' est d'ordre multiple de 8 et puisqu'il est cyclique, la restriction de x' à L est égale à 1. Il en sera de même de x'' . Puisque G'' est aussi cyclique, x'' est un carré et G'' est d'ordre divisible par 16. Nous avons donc montré que $h(-2p) \equiv 0 \pmod{16}$.

L'implication B résulte des deux propositions énoncées ci-dessus et de l'implication: $h(2p) \equiv 0 \pmod{8} \Rightarrow h(-p) \equiv 0 \pmod{8}$ ([3]).

III. Conjecture et contre-exemples.

Les trois implications suivantes sont fausses. On a écrit à la suite de chacune d'elles le plus petit p qui les contredit :

$$h(2p) \equiv 0 \pmod{16} \Rightarrow h(-p) \equiv 0 \pmod{16}; \quad (2593)$$

$$h(-p) \equiv 0 \pmod{16} \text{ et } h(-2p) \equiv 0 \pmod{16} \Rightarrow h(2p) \equiv 0 \pmod{16}; \quad (257)$$

$$h(2p) \equiv 0 \pmod{32} \Rightarrow h(-2p) \equiv 0 \pmod{32}; \quad (12641)$$

P. Kaplan a suggéré de préciser l'implication B par la conjecture suivante : Si $h(2p) \equiv 0 \pmod{8}$, alors : $h(-2p) \equiv 0 \pmod{16}$ si et seulement si $h(2p) \equiv 0 \pmod{16}$ ou l'équation $x^2 - 2py^2 = -2$ a des solutions entières.

Bibliographie

- [1] G. Gras, Sur les l -classes d'idéaux dans les extensions cycliques relatives de degré premier l , Ann. Inst. Fourier, 23 (1973).
- [2] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie Verlag, Berlin, 1952.
- [3] P. Kaplan, Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique et réciprocity biquadratique, J. Math. Soc. Japan, 25 (1973), 596-608.
- [4] P. Kaplan et C. Sanchez, Table des 2-groupes des classes d'idéaux au sens restreint et des facteurs principaux des corps quadratiques réels $\mathbb{Q}(\sqrt{2p})$, $p < 2 \cdot 10^6$, Université de Nancy I (1974).
- [5] H. W. Leopoldt, Zur Struktur der l -Klassengruppe galoischer Zahlkörper, J. Reine Angew. Math., 199 (1958) 165-175.
- [6] B. Oriat, Relations entre les 2-groupes des classes d'idéaux des extensions quadratiques $k(\sqrt{d})$ et $k(\sqrt{-d})$, Ann. Inst. Fourier, 27 (1977) (à paraître).
- [7] B. Oriat, Spiegelungssatz, Publications mathématiques de la Faculté de Besançon, 1975.

Bernard ORIAT
 Faculté des Sciences
 Mathématiques
 Université de Besançon
 25030 Besançon Cedex
 France

Un essai de généralisation du «Spiegelungssatz»

Par Bernard Oriat à Besançon et Philippe Satgé à Caen

Introduction

Le «Spiegelungssatz» démontré par Leopoldt dans [9] généralise des énoncés plus anciens comme celui de Kummer: «Si le nombre de classes réelles du corps cyclotomique $\mathbb{Q}^{(l)}$ est divisible par l , alors le nombre de classes relatives de ce corps est aussi divisible par l », ou celui de Scholtz [15] liant les 3-ranges des groupes de classes d'idéaux des corps quadratiques $\mathbb{Q}(\sqrt{\alpha})$ et $\mathbb{Q}(\sqrt{-3\alpha})$. Leopoldt considère un nombre premier l , une extension galoisienne L/k de corps de nombres et suppose d'une part que L contient les racines de l'unité d'ordre l et d'autre part, que l ne divise pas le degré de L/k . A chaque caractère Φ du groupe $G = \text{Gal}(L/k)$ irréductible sur le corps l -adique $\mathbb{Q}_l$, il associe un groupe de classes d'idéaux $\mathcal{H}_\Phi$ d'un sous-corps K_Φ de L . Enfin, il définit une involution sur l'ensemble des caractères et note $\bar{\Phi}$ l'image de Φ par cette involution. Il donne alors un majorant de la différence des l -rangs des groupes $\mathcal{H}_{\bar{\Phi}}$ et $\mathcal{H}_\Phi$. Le changement de Φ en $\bar{\Phi}$ permutant $\mathcal{H}_\Phi$ et $\mathcal{H}_{\bar{\Phi}}$, on en déduit un minorant de cette différence.

Nous essayons dans ce travail de donner des majorations et des minoration analogues à celles énoncées par Leopoldt, sans utiliser l'hypothèse de non divisibilité par l du degré de L/k . Pour cela nous devons exclure le cas $l=2$. Nous fixons une puissance de l que nous notons n , nous supposons que L contient les racines $n^{\text{ièmes}}$ de l'unité et que l'extension L/k est abélienne. Les groupes de classes que nous considérons sont associés, non plus à des caractères du groupe de Galois G de l'extension L/k , mais à des idéaux de l'algèbre $A_n[G]$, où A_n désigne l'anneau des entiers modulo n . Sur l'ensemble de ces idéaux nous définissons une involution du même type que celle définie par Leopoldt. A chaque idéal I nous associons deux groupes de classes d'idéaux $\mathcal{H}_I$ et $\mathcal{H}^I$ d'un sous-corps K_I de L . Nous notons $\bar{I}$ l'image de I par notre involution. Pour toute puissance de l , notée m , comprise entre l et n , nous donnons des majorations et des minoration de la différence des m -rangs des groupes $\mathcal{H}^{\bar{I}}$ et $\mathcal{H}_I$. Ici, les groupes $\mathcal{H}_I$ et $\mathcal{H}^I$ étant distincts, le changement de I en $\bar{I}$ ne permute pas $\mathcal{H}_I$ et $\mathcal{H}^{\bar{I}}$ et les minoration ne résultent pas des majorations, non plus qu'inversement.

Les majorations obtenues sont données dans le théorème 1. Suivant que certaines hypothèses sont ou ne sont pas vérifiées nous obtenons une inégalité plus ou moins précise, mais nous obtenons toujours une inégalité. Si l ne divise pas le degré de $[L:k]$, ce théorème redonne le «Spiegelungssatz» de Leopoldt (à ceci près que nous supposons l impair et L/k abélienne; le cas $l=2$ a d'ailleurs fait l'objet d'autres études [10] et [11]).

Les minorations sont énoncées dans le théorème 2. Leurs démonstrations sont plus délicates et ne sont obtenues que sous certaines hypothèses restrictives.

L'essentiel des résultats obtenus est énoncé dans les théorèmes 1 et 2 (§ 1). On trouvera les démonstrations dans les paragraphes 2, 3, 4 et 5. On a donné dans les paragraphes suivants quelques illustrations des définitions et des inégalités obtenues.

1. Définitions. notations. énoncé des principaux résultats

Soit m un entier. Si K est un corps de caractéristique 0, on désigne par $K^{(m)}$ le corps obtenu en adjoignant à K une racine primitive $m^{\text{ème}}$ de 1. D'autre part, si H est un groupe abélien, on désigne par $H^{(m)}$ le sous-groupe de H formé des éléments dont l'ordre divise m et par H^m le sous-groupe des puissances $m^{\text{èmes}}$ d'éléments de H .

Soient l un nombre premier impair et n une puissance de l . On choisit une racine primitive $n^{\text{ème}}$ de 1 que l'on note ζ . On désigne par L/k une extension abélienne finie de corps de nombres et par G son groupe de Galois. On suppose que L contient ζ , c'est-à-dire que $L = L^{(n)}$.

On note A_n l'anneau des classes résiduelles modulo n , c'est-à-dire $A_n = \mathbb{Z}/n\mathbb{Z}$ et A_n^* le groupe multiplicatif de cet anneau. Pour tout τ de G nous désignons par $\chi^*(\tau)$ la classe résiduelle modulo n telle que $\zeta^\tau = \zeta^{\chi^*(\tau)}$. On définit ainsi un homomorphisme de groupes de G dans A_n^* .

Considérons maintenant l'algèbre $A_n[G]$ du groupe G , à coefficients dans A_n . Si $x = \sum_{\tau \in G} a_\tau \tau$ est un élément de $A_n[G]$, nous posons $\bar{x} = \sum_{\tau \in G} a_\tau \chi^*(\tau) \tau^{-1}$. L'application de $A_n[G]$ dans lui-même qui à x fait correspondre $\bar{x}$ est un automorphisme involutif de $A_n[G]$. Si I est un idéal de $A_n[G]$, on note $\bar{I}$ l'image de I par cette involution.

D'une façon générale, pour tout groupe H et tout idéal J de $A_n[H]$, on appelle noyau de J l'ensemble des τ de H tels que $\tau - 1$ appartienne à J . C'est un sous-groupe de H que l'on note $\text{Ker } J$.

On désigne toujours par I un idéal de $A_n[G]$. On note K_I le corps intermédiaire entre L et k invariant par $\text{Ker } I$. On pose $G_I = G/\text{Ker } I$ et on identifie ce groupe à $\text{Gal}(K_I/k)$. On désigne par I' l'image de I par la surjection canonique de $A_n[G]$ sur $A_n[G_I]$. Le noyau de l'idéal I' est trivial. De plus l'application qui à I fait correspondre I' est une bijection de l'ensemble des idéaux de $A_n[G]$ de noyau égal à $\text{Gal}(L/K_I)$ sur l'ensemble des idéaux de $A_n[G_I]$ de noyau trivial. On peut donc se donner à priori, l'extension abélienne K_I/k , un idéal I' de $A_n[\text{Gal}(K_I/k)]$ de noyau trivial et un corps L contenant $K_I^{(n)}$ et abélien sur k (par exemple $L = K_I^{(n)}$). L'idéal I de $A_n[G]$ est alors défini comme l'image réciproque de I' par la surjection canonique de $A_n[G]$ sur $A_n[\text{Gal}(K_I/k)]$.

Soit $\mathcal{H}(K_I)$ le l -groupe des classes d'idéaux de K_I . Nous notons $\mathcal{H}(K_I)^{I'}$ le sous-groupe de $\mathcal{H}(K_I)$ contenant $[\mathcal{H}(K_I)]^n$ et engendré par les éléments de la forme h^x , où h appartient à $\mathcal{H}(K_I)$ et x appartient à I' (dans la notation h^x , x est confondu avec un relèvement de x dans $\mathbb{Z}[G]$). Nous posons $\mathcal{H}^I = \mathcal{H}(K_I)/\mathcal{H}(K_I)^{I'}$. Le groupe $\mathcal{H}^I$ est donc le plus grand quotient de $\mathcal{H}(K_I)/[\mathcal{H}(K_I)]^n$ annulé par l'idéal I' .

D'autre part, nous notons $\mathcal{H}_I$ le plus grand sous-groupe de $\mathcal{H}(K_I)$ annulé par n et I' . C'est-à-dire que $\mathcal{H}_I$ est l'ensemble des h de $\mathcal{H}(K_I)$ tels que $h^n = 1$ et $h^x = 1$ pour tout x de I' .

Remarque 1. 1. Il n'y a pas, à notre connaissance, de relation simple entre $\mathcal{H}^I$ et $\mathcal{H}_I$. Toutefois, si l'idéal I' est principal, alors $\mathcal{H}^I$ est nul si et seulement si $\mathcal{H}_I$ est nul. En effet, désignons par i un relèvement quelconque d'un générateur de I' dans $\mathbb{Z}[G_I]$, par $\mathcal{H}(K_I)^{(i)}$ l'ensemble des h de $\mathcal{H}(K_I)$ annulés par i et par $\mathcal{H}(K_I)^i$ l'image de $\mathcal{H}(K_I)$ par l'action de i . Montrons que $\mathcal{H}_I$ est nul si et seulement si $\mathcal{H}(K_I)^{(i)}$ est nul : il est clair que $\mathcal{H}_I$ est nul si $\mathcal{H}(K_I)^{(i)}$ l'est ; d'autre part, si $h \neq 1$ est dans $\mathcal{H}(K_I)^{(i)}$, alors la plus petite puissance de h dont l'ordre est divisible par n est un élément non nul de $\mathcal{H}_I$, d'où notre assertion. De même, $\mathcal{H}^I$ est trivial si et seulement si $\mathcal{H}(K_I)/\mathcal{H}(K_I)^i$ est trivial : en effet, il est clair que $\mathcal{H}^I$ est nul si $\mathcal{H}(K_I)/\mathcal{H}(K_I)^i$ l'est ; d'autre part, si h est un élément de $\mathcal{H}(K_I)$ dont la classe dans $\mathcal{H}(K_I)/\mathcal{H}(K_I)^i$ est non nulle, alors ou bien sa classe dans $\mathcal{H}^I$ est non nulle et c'est fini, ou bien $h = k_1^i h_1^n$ pour deux éléments k_1 et h_1 de $\mathcal{H}(K_I)$; la classe de h_1 dans $\mathcal{H}(K_I)/\mathcal{H}(K_I)^i$ est non nulle (car sinon celle de h le serait) et on recommence le raisonnement avec h_1 ; il est clair qu'en un nombre fini d'étapes, on trouve un élément dont la classe dans $\mathcal{H}^I$ est non nulle, ce qui prouve notre assertion. On conclut alors cette remarque en considérant la suite exacte

$$1 \rightarrow \mathcal{H}(K_I)^{(i)} \rightarrow \mathcal{H}(K_I) \rightarrow \mathcal{H}(K_I)^i \rightarrow 1$$

qui montre que $\mathcal{H}(K_I)^{(i)}$ est nul si et seulement si $\mathcal{H}(K_I)/\mathcal{H}(K_I)^i$ l'est.

Soient maintenant $E(K_I)$ le groupe des unités de K_I et $\mathcal{E}(K_I)$ le quotient de $E(K_I)$ par le sous-groupe de ses puissances $n^{\text{ièmes}}$ i.e. $\mathcal{E}(K_I) = E(K_I)/E(K_I)^n$. Il s'agit d'un $A_n[G_I]$ -module ; nous désignons par $\mathcal{E}_I$ le plus grand sous-module de $\mathcal{E}(K_I)$ annulé par I' , c'est-à-dire l'ensemble des ε de $\mathcal{E}(K_I)$ tels que $\varepsilon^x = 1$ pour tout x de I' . Nous désignons aussi par $\mathcal{E}_I^0$ l'ensemble des ε de $\mathcal{E}_I$ qui sont n -primaires sur K_I , c'est-à-dire telles que l'extension $K_I^{(n)}(\sqrt[n]{\varepsilon})/K_I^{(n)}$ est non ramifiée ; c'est un sous- $A_n[G_I]$ -module de $\mathcal{E}_I$.

Enfin, si H est un groupe abélien et si m est une puissance de l , on note $\dim_m H$ le m -rang de H (c'est-à-dire la dimension sur le corps à l éléments $\mathbb{F}_l$ du quotient $(H^{(m)})/(H^{(m/l)})$).

Comme nous l'avons dit dans l'introduction nous aurons besoin, pour énoncer les deux théorèmes fondamentaux de ce travail, de privilégier un certain nombre de situations. Pour le théorème 1, introduisons trois hypothèses notées A_1 , B_1 et C_1 :

A_1) Le degré de l'extension $K_I^{(n)}/K_I$ est premier à l .

B_1) Le corps K_I ne contient pas de racine de l'unité d'ordre l .

C_1) Il existe un idéal premier de K_I totalement ramifié dans $K_I^{(n)}/K_I$ (les idéaux étrangers à l ne se ramifiant pas dans $K_I^{(n)}/K_I$, cet idéal contient l).

Le théorème 1 s'énonce alors :

Théorème 1. Soit m une puissance de l comprise entre l et n . On a toujours l'inégalité

$$\dim_m \mathcal{H}^I - \dim_m \mathcal{H}_I \leq \dim_l \mathcal{E}_I^0 + 1 ;$$

si de plus l'une des hypothèses A_1 , B_1 ou C_1 est vérifiée, on a l'inégalité plus forte

$$\dim_m \mathcal{H}^I - \dim_m \mathcal{H}_I \leq \dim_l \mathcal{E}_I^0 .$$

Ce théorème est conséquence immédiate du théorème 1' énoncé à la fin du paragraphe 4 ; on y donne l'inégalité $\dim_m \mathcal{H}^I - \dim_m \mathcal{H}_I \leq \dim_l \mathcal{E}_I^0$ sous une hypothèse plus faible que A_1 , B_1 ou C_1 .

Pour le théorème 2, nous devons introduire les idéaux premiers $l_1, \dots, l_t$ de $K_I \cap K_{\bar{I}}$ au dessus de l . Pour tout j de 1 à t , on choisit un idéal premier $\mathfrak{Q}_j$ de K_I au dessus de l_j et on désigne par U_j le groupe des unités principales du complété de K_I en $\mathfrak{Q}_j$, par D_j le groupe de décomposition de $\mathfrak{Q}_j$ dans $K_I \cdot k$ et par $I(j)$ l'intersection de I' avec $A_n[D_j]$. Le quotient U_j/U_j^n est un $A_n[D_j]$ -module et nous notons $\mathcal{U}_{I(j)}$ le plus grand sous-module de U_j/U_j^n annulé par $I(j)$. Enfin nous introduisons quatre hypothèses notées A_2, B_2, B'_2 et C_2 :

A_2) Le degré de l'extension K_I/k est premier à l et l'idéal I' est engendré par un idempotent de l'algèbre $A_n[G_I]$.

B_2) Le corps K_I ne contient pas de racine de l'unité d'ordre l et, si $(K_{\bar{I}})_0$ désigne la plus grande extension de $K_I \cap K_{\bar{I}}$ de degré premier à l contenue dans $K_{\bar{I}}$, alors aucun idéal premier de $K_I \cap K_{\bar{I}}$ divisant l n'est totalement décomposé dans $(K_{\bar{I}})_0$.

B'_2) Le corps K_I ne contient pas de racine de l'unité d'ordre l et l'extension $K_I^{(n)}/K_{\bar{I}}$ est modérément ramifiée.

C_2) Il existe un idéal premier et un seul de $K_{\bar{I}}$ qui est totalement ramifié dans $K_I^{(n)}/K_{\bar{I}}$ (il n'y a alors qu'un seul idéal premier de $K_{\bar{I}}$ au dessus de l et c'est lui qui est totalement ramifié).

Remarque 1. 2. A l'aide du lemme 3. 1 du § 3, on montre que A_2 implique A_1 ; d'autre part, il est clair que chacune des hypothèses B_2 et B'_2 implique B_1 et que C_2 implique C_1 .

Le théorème 2 s'énonce alors de la manière suivante:

Théorème 2. Soit m une puissance de l comprise entre l et n . Si l'hypothèse A_2 est vérifiée, alors on a l'inégalité:

$$\dim_m \mathcal{E}_I - \sum_{j=1}^t \dim_l \mathcal{U}_{I(j)} \leq \dim_m \mathcal{H}^{\bar{I}} - \dim_m \mathcal{H}_I.$$

Si l'une des hypothèses B_2, B'_2 ou C_2 est vérifiée, alors en désignant par s le nombre minimal de générateurs de I' on a l'inégalité:

$$- \sum_{j=1}^t \dim_l \mathcal{U}_{I(j)} - s \dim_l \mathcal{E}(K_I) + \dim_m \mathcal{E}(K_I) \leq \dim_m \mathcal{H}^{\bar{I}} - \dim_m \mathcal{H}_I.$$

Ce théorème 2 est une partie du théorème 2' démontré au paragraphe 5. Dans ce théorème 2' nous montrons que, si un certain homomorphisme A_I (défini au paragraphe 5) est surjectif, alors on peut remplacer la dernière inégalité du théorème 2 par l'inégalité

$$- \sum_{j=1}^t \dim_l \mathcal{U}_{I(j)} \leq \dim_m \mathcal{H}^{\bar{I}} - \dim_m \mathcal{H}_I.$$

Si $s=1$ cette amélioration est peu sensible; en effet les quantités $\dim_l \mathcal{E}(K_I)$ et $\dim_m \mathcal{E}(K_I)$ sont égales à une unité près au rang de la partie libre du groupe des unités de K_I . Si par contre s est strictement plus grand que 1, alors la quantité

$$s \dim_l \mathcal{E}(K_I) - \dim_m \mathcal{E}(K_I)$$

semble plus grande que les autres termes de l'inégalité et cette amélioration est plus sensible. Malheureusement le domaine de validité de cette hypothèse de surjectivité nous paraît mal connue.

2. Lemmes

On trouve le lemme suivant dans [2]:

Lemme 2. 1. Soit K un corps de caractéristique 0 et n une puissance du nombre impair l . Alors toute puissance $n^{\text{ème}}$ d'un élément de $K^{(n)}$ appartenant à K est une puissance $n^{\text{ème}}$ d'un élément de K . Soit, en abrégé $[K^{(n)}]^n \cap K = K^n$. *premier*

Démonstration. Désignons toujours par ζ une racine primitive $n^{\text{ème}}$ de 1. Distinguons deux cas, suivant que K contient ou non une racine primitive $l^{\text{ème}}$ de 1. Supposons d'abord que K ne contient pas une telle racine. Soit χ l'homomorphisme injectif de $\text{Gal}(K^{(n)}/K)$ dans A_n^* défini par $\zeta^{\chi(\tau)} = \zeta^\tau$ pour tout τ de $\text{Gal}(K^{(n)}/K)$. Soit σ un générateur de $\text{Gal}(K^{(n)}/K)$. Puisque $K^{(l)} \neq K$, la quantité $\chi(\sigma) - 1$ n'est pas multiple de l et est donc inversible. Toute racine $n^{\text{ème}}$ de 1 peut donc se mettre sous la forme $\zeta^{\sigma^{-1}}$, où ζ est une autre racine $n^{\text{ème}}$ de 1. Soit maintenant u appartenant à $K^{(n)}$ et tel que u^n appartienne à K . Alors $u^{\sigma^{-1}}$ est une racine $n^{\text{ème}}$ de 1. Nous pouvons donc écrire $u^{\sigma^{-1}} = \zeta^{\sigma^{-1}}$ et, si $u' = u\zeta^{\sigma^{-1}}$, nous avons $u'^n = u^n$ avec u' dans K .

Supposons maintenant que K contient une racine $l^{\text{ème}}$ de 1. Soit toujours u un élément de $K^{(n)}$ tel que u^n appartienne à K . Puisque $[K(u):K] \leq \varphi(n)$, le polynôme $X^n - u^n$ est réductible sur K et il s'en suit que u^n appartient à K^l ([8] ch. VIII § 9), donc $u^{n/l}$ appartient à K . Si u appartient à $K^{(n/l)}$, alors nous sommes ramenés au même problème, où n/l remplace n . Supposons que u n'appartienne pas à $K^{(n/l)}$. Alors dans ce cas on a $K^{(n/l)}(u) = K^{(n)}$, c'est-à-dire $K^{(n/l)}(\sqrt[n/l]{u^{n/l}}) = K^{(n/l)}(\sqrt[n/l]{\zeta^{n/l}})$. Comme on le sait cela implique l'existence d'un entier naturel x et d'un u_1 dans $K^{(n/l)}$ tel que $u^{n/l} = (\zeta^{n/l})^x u_1^{n/l}$; on a donc $u_1^n = u^n$ et $u_1^{n/l}$ est dans K . Nous sommes donc revenu au problème initial, où cette fois, n est remplacé par n/l et u par u_1 .

Lemme 2. 2. On désigne par m une puissance de l . Soient A , B et C trois groupes abéliens s'insérant dans une suite exacte $1 \rightarrow A \rightarrow B \rightarrow C$; alors on a les inégalités:

$$\dim_m B - \dim_m A \leq \dim_l C; \quad \text{et} \quad \dim_m B - \dim_m C \leq \dim_l A.$$

Démonstration. Soit φ l'homomorphisme de B dans C . A partir de la suite exacte donnée on forme les suites exactes:

$$1 \rightarrow A^{(m)} \rightarrow B^{(m)} \rightarrow C^{(m)},$$

$$1 \rightarrow A^{(m)} B^{(m/l)} / B^{(m/l)} \rightarrow B^{(m)} / B^{(m/l)} \rightarrow C^{(m)} / \varphi(B^{(m/l)}).$$

Or $A^{(m)} B^{(m/l)} / B^{(m/l)}$ est isomorphe à $A^{(m)} / A^{(m/l)}$. D'où l'on tire

$$\dim_m B - \dim_m A \leq \dim_l C^{(m)} / \varphi(B^{(m/l)}) \leq \dim_l C.$$

D'autre part, à partir de $1 \rightarrow A^{(m)} \rightarrow B^{(m)} \rightarrow C^{(m)}$ nous pouvons former la suite exacte:

$$1 \rightarrow A^{(m)} \cap [B^{(m)}]^{m/l} \rightarrow [B^{(m)}]^{m/l} \rightarrow [C^{(m)}]^{m/l}.$$

Mais on a $\dim_m B = \dim_l [B^{(m)}]^{m/l}$ et $\dim_m C = \dim_l [C^{(m)}]^{m/l}$ d'où:

$$\dim_m B - \dim_m C \leq \dim_l (A^{(m)} \cap [B^{(m)}]^{m/l}) \leq \dim_l A.$$

Lemme 2. 3. *On désigne toujours par m une puissance de l . Soient A, B, C des l -groupes abéliens finis. Si la suite*

$$1 \rightarrow A \rightarrow B \rightarrow C \rightarrow 1$$

est exacte et si $A \cap B^m = A^m$, alors:

$$\dim_m B \geq \dim_m A + \dim_m C.$$

Démonstration. A partir de la suite exacte donnée, on forme:

$$1 \rightarrow A \cap B^{m/l} \rightarrow B^{m/l} \rightarrow C^{m/l} \rightarrow 1$$

et en passant aux quotients:

$$1 \rightarrow [(A \cap B^{m/l}) B^m] / B^m \rightarrow B^{m/l} / B^m \rightarrow C^{m/l} / C^m \rightarrow 1.$$

Le premier groupe est isomorphe à $(A \cap B^{m/l}) / (A \cap B^m) = (A \cap B^{m/l}) / A^m$ et a pour sous-groupe $A^{m/l} / A^m$, d'où la relation annoncée.

3. Début de la démonstration des théorèmes

Soit I un idéal de $A_n[G]$; dans toute la suite nous supposons que l'intersection de I et de A_n est réduite à 0 (on peut vérifier que cela ne restreint pas la généralité des théorèmes 1 et 2). Cette hypothèse permet de démontrer le lemme suivant:

Lemme 3. 1. *Les corps $K_I^{(n)}$, $K_{\bar{I}}^{(n)}$ et $K_I K_{\bar{I}}$ coïncident. De plus, on ne modifie aucune des définitions introduites précédemment ($\bar{I}$, $\mathcal{H}_I$, $\mathcal{H}^{\bar{I}}$, $\mathcal{E}_I$, $\mathcal{U}_{I(j)}$) en supposant que $L = K_I^{(n)}$; nous le ferons donc dans la suite.*

Définition de N . Soit $N/K_{\bar{I}}$ l'extension abélienne non ramifiée maximale qui correspond par la théorie du corps de classes à $\mathcal{H}^{\bar{I}}$. Faisons opérer $G_{\bar{I}}$ sur $\text{Gal}(N/K_{\bar{I}})$ par conjugaison, c'est-à-dire: si τ appartient à $G_{\bar{I}}$ et si t est un prolongement de τ à N , on pose $u^t = t^{-1} u t$ pour tout u de $\text{Gal}(N/K_{\bar{I}})$. Rappelons que l'isomorphisme de réciprocity $\text{Gal}(N/K_{\bar{I}}) \cong \mathcal{H}^{\bar{I}}$ est un isomorphisme de $A_n[G_{\bar{I}}]$ -modules (à droite).

Définition de M et W . Nous poserons $M = NL$. Comme M/L est d'exposant divisant n et que L contient les racines $n^{\text{èmes}}$ de 1, cette extension est une extension de Kummer. On désignera par W son radical. C'est-à-dire $W = \{w; w \in L^*; \sqrt[n]{w} \in M\}$.

Lemme 3. 2. *On a des isomorphismes de groupes, $\mathcal{H}^{\bar{I}} \cong \text{Gal}(N/K_{\bar{I}})$ et $\text{Gal}(M/L) \cong W/L^{*n}$. Si l'intersection $N \cap L$ est égale à $K_{\bar{I}}$, on a un isomorphisme $\text{Gal}(N/K_{\bar{I}}) \cong \text{Gal}(M/L)$. Sinon on a quand même:*

$$0 \leq \dim_m \text{Gal}(N/K_{\bar{I}}) - \dim_m \text{Gal}(M/L) \leq 1,$$

pour toute puissance de l , notée m et telle que $l \leq m \leq n$.

Démonstration. Le premier isomorphisme cité est l'isomorphisme de réciprocity du corps de classes, le deuxième est l'isomorphisme classique de la théorie de Kummer. Si $N \cap L = K_{\bar{I}}$, il est clair que les groupes de Galois de $N/K_{\bar{I}}$ et M/L sont isomorphes. Sinon, on considère la suite exacte:

$$1 \rightarrow \text{Gal}(M/L) \rightarrow \text{Gal}(N/K_{\bar{I}}) \rightarrow \text{Gal}(N \cap L/K_{\bar{I}})$$

dont le dernier terme est cyclique. On déduit l'inégalité annoncée du lemme 2. 2.

Comme N/k est galoisienne, il en est de même de M/k . Il s'en suit que W/L^{*n} est un $A_n[G]$ -module. D'autre part, on fait également opérer G sur $\text{Gal}(M/L)$ par conjugaison. Ces deux groupes ne sont pas isomorphes en tant que G -modules, mais leurs structures sont liées par la «Spiegelungsrelation» ([9] ou [4]) que nous rappelons :

Proposition 3. 3. *Soit α l'isomorphisme classique de la théorie de Kummer de W/L^{*n} sur le dual de $\text{Gal}(M/L)$. Il est défini par $\alpha(wL^{*n})(u) = (\sqrt[n]{w})^{u-1}$, w étant un élément de W et u un élément de $\text{Gal}(M/L)$. Alors, pour tout x de $A_n[G]$, on a l'égalité :*

$$[\alpha(wL^{*n})](u^x) = [\alpha((wL^{*n})^x)](u).$$

Démonstration. Posons $\varrho = \sqrt[n]{w}$ et $\tilde{w} = wL^{*n}$ pour simplifier les notations. Désignons par τ un élément de G et par t un prolongement de τ à M . D'après la définition de w nous avons $[\alpha(\tilde{w})(u^\tau)]\varrho = \varrho^{u^\tau}$. D'autre part, on a aussi : $\varrho^{t^{-1}u} = [\alpha(\tilde{w}^{t^{-1}})(u)]\varrho^{t^{-1}}$, d'où l'on déduit

$$\varrho^{u^\tau} = \varrho^{t^{-1}ut} = [\alpha(\tilde{w}^{t^{-1}})(u)\varrho^{t^{-1}}]^t = [\alpha(\tilde{w}^{t^{-1}})(u)]^\tau \varrho.$$

Mais, $[\alpha(\tilde{w})^{t^{-1}}](u)$ est une racine $n^{\text{ème}}$ de 1. Donc son image par τ est égale à sa puissance $\chi^*(\tau)^{\text{ème}}$. Nous avons donc

$$\varrho^{u^\tau} = \alpha(\tilde{w}^{\chi^*(\tau)^{-1}})(u)\varrho$$

d'où l'égalité :

$$\alpha(\tilde{w})(u^\tau) = \alpha(\tilde{w}^{\chi^*(\tau)^{-1}})(u) = \alpha(\tilde{w}^\tau)(u).$$

Corollaire 3. 4. *L'idéal I de $A_n[G]$ annule W/L^{*n} .*

Démonstration. Considérons $\text{Gal}(N/K_I)$: c'est un $A_n[G_I]$ -module, donc un $A_n[G]$ -module aussi. Le sous-groupe $\text{Gal}(N/N \cap L)$ en est un sous-module isomorphe à $\text{Gal}(M/L)$. Il s'en suit puisque $\bar{I}$ annule $\text{Gal}(N/K_I)$, que $\bar{I}$ annule aussi $\text{Gal}(M/L)$. D'après la proposition précédente, I annule W/L^{*n} .

Définition de W' . On pose $W' = W \cap K_I$.

Lemme 3. 5. *L'injection canonique de W' dans W induit un isomorphisme de $A_n[G]$ -modules $W'/K_I^{*n} \cong W/L^{*n}$. De plus, W'/K_I^{*n} est un $A_n[G_I]$ -module.*

Démonstration. Considérons l'application de W' dans W/L^{*n} qui associe à w appartenant à W' la classe de w modulo L^{*n} . Cet homomorphisme a pour noyau $W' \cap L^{*n} = W' \cap K_I \cap L^{*n} = K_I^{*n}$ d'après le lemme 2. 1. Montrons qu'il est surjectif. Soit w un élément de W et σ un générateur de $\text{Ker } I = \text{Gal}(L/K_I)$. D'après le corollaire précédent, $(wL^{*n})^{\sigma-1} = 1$ et il existe β dans L tel que $w^{\sigma-1} = \beta^n$. Considérons maintenant $N_{L/K_I}(\beta)$. C'est une racine $n^{\text{ème}}$ de 1 appartenant à K_I .

Si K_I ne contient pas de racine primitive $l^{\text{ème}}$ de 1, alors $N_{L/K_I}(\beta)$ est égal à 1. A l'opposé si $K_I = K_I^{(m)}$, alors le lemme est évident. Supposons donc $K_I = K_I^{(m)} \neq K_I^{(ml)}$ avec $l \leq m \leq n/l$. Nous avons alors $\chi^*(\sigma) \equiv 1(m)$ et $\chi^*(\sigma) \not\equiv 1(ml)$. L'ensemble $\chi^*(\text{Ker } I)$ est donc l'ensemble des classes résiduelles modulo n congrues à 1 modulo m , d'où $N_{L/K_I}(\zeta) = \zeta^{\sum (1+\mu m)}$ avec $0 \leq \mu \leq n/m - 1$. La somme $\sum \mu$ est congrue à 0 modulo n/m et il reste $N_{L/K_I}(\zeta) = \zeta^{n/m}$. Cette dernière quantité est une racine primitive $m^{\text{ème}}$ de 1, donc $N_{L/K_I}(\beta)$ est une puissance de $\zeta^{n/m}$ et on peut remplacer β par β' tel que $N_{L/K_I}(\beta') = 1$ et $w^{\sigma-1} = \beta'^n$. Le théorème 90 de Hilbert montre que β est de la forme $\gamma^{\sigma-1}$ avec γ dans L . Posant $w' = \gamma^{-n}w$, nous constatons que $w'L^{*n}$ est égal à wL^{*n} et que w' se trouve dans W' .

Il est clair que l'isomorphisme ci-dessus est un isomorphisme de $A_n[G]$ -modules. De plus, comme ces modules sont annihilés par I , ils sont invariants par $\text{Ker } I$. Ce sont donc des modules sur $A_n[G_I]$.

4. Fin de la démonstration du théorème 1

Proposition 4. 1. *Si w appartient à W' , alors l'idéal de K_I engendré par w est la puissance $n^{\text{ème}}$ d'un idéal de K_I .*

Démonstration. Soit donc w un élément de W' . Comme l'extension de Kummer $L(\sqrt[n]{w})/L$ est non ramifiée, w engendre dans L un idéal qui est une puissance $n^{\text{ème}}$ (d'un idéal de L). Décomposons cet idéal en produit de deux idéaux, $\mathfrak{A}_1$ premier à l et $\mathfrak{A}_2$ divisible seulement par des idéaux au-dessus de l . Nous avons donc (A_L étant l'anneau des entiers de L):

$$wA_L = \mathfrak{A}_1^n \mathfrak{A}_2^n.$$

Comme w appartient à K_I , $\mathfrak{A}_1$ et $\mathfrak{A}_2$ sont invariants par $\text{Gal}(L/K_I)$. D'autre part, seuls les idéaux au-dessus de l peuvent être ramifiés dans L/K_I . Il s'en suit que $\mathfrak{A}_1$ est l'étendu d'un idéal de K_I .

Pour montrer qu'il en est de même de $\mathfrak{A}_2$ introduisons un idéal $\mathfrak{Q}$ de K_I au-dessus de l et un complété $\hat{K}_I$ de K_I pour cet idéal $\mathfrak{Q}$. Il suffit de montrer que l'idéal engendré par w dans $\hat{K}_I$ est une puissance $n^{\text{ème}}$ de $\mathfrak{Q}$.

Soit $\hat{L}$ un complété de L pour un idéal au-dessus de $\mathfrak{Q}$. Introduisons T_0 corps d'inertie de l'extension $\hat{L}/\hat{K}_I$ et T_1 corps d'inertie de l'extension $\hat{L}(\sqrt[n]{w})/T_0$. Soit n_0 la plus grande puissance de l , telle que $\hat{K}_I^{(n_0)} = \hat{K}_I$. Si $n = n_0$, l'idéal $\mathfrak{Q}$ n'est pas ramifié dans L/K_I et la proposition est claire. Sinon il existe τ dans $\text{Gal}(\hat{L}/\hat{K}_I)$ tel que

$$\chi^*(\tau) \equiv 1(n_0) \quad \text{et} \quad \chi^*(\tau) \not\equiv 1(n_0 l).$$

D'autre part, le corollaire 3. 4 montre que $\text{Gal}(L/K_I)$ agit trivialement sur W/L^{*n} , donc l'extension $L(\sqrt[n]{w})/K_I$ est galoisienne. Il en est donc de même de $\hat{L}(\sqrt[n]{w})/\hat{K}_I$. Mais de plus, comme T_1 est le corps d'inertie de cette extension, $T_1/\hat{K}_I$ est cyclique. Il en est de même de $\hat{L}/\hat{K}_I$ et donc la composée de ces deux extensions est abélienne; cette composée est $\hat{L}(\sqrt[n]{w})/\hat{K}_I$ puisque $\hat{L}(\sqrt[n]{w})/\hat{L}$ est non ramifiée.

Soit u appartenant à $\text{Gal}(\hat{L}(\sqrt[n]{w})/\hat{L})$. Les groupes de Galois des extensions locales sont des sous-groupes des groupes de Galois des extensions globales correspondantes. Nous pouvons donc dire que $\tau - 1$ appartient à I , donc $\tau - \chi^*(\tau)$ appartient à $\bar{I}$ et on a $u^\tau = u^{\chi^*(\tau)}$. Mais on a aussi $u^\tau = u$ puisque $\hat{L}(\sqrt[n]{w})/\hat{K}_I$ est abélienne. Il s'en suit que $u^{1-\chi^*(\tau)} = 1$, c'est-à-dire $u^{n_0} = 1$. Le degré de $\hat{L}(\sqrt[n]{w})/\hat{L}$ est donc inférieur à n_0 . Il en est de même du degré de T_1/T_0 ; mais T_0 contient les racines $n_0^{\text{èmes}}$ de 1, donc l'extension T_1/T_0 est une extension de Kummer; il existe donc un w_0 dans T_0 tel que $T_1 = T_0(\sqrt[n_0]{w_0})$. Puisque $\hat{L}(\sqrt[n]{w})$ est la composée de $\hat{L}$ et de T_1 , on a $\hat{L}(\sqrt[n]{w}) = \hat{L}(\sqrt[n]{w_0^{n/n_0}})$ et donc il existe un entier p premier à l et un c dans $\hat{L}$ tels que $w = (w_0^{n/n_0})^p c^n$. De cette égalité résulte que c^n appartient à T_0 ; on déduit donc du lemme 2. 1 (appliqué à T_0) qu'il existe c_0 dans T_0 tel que $c^n = c_0^n$ et on a $w = (w_0^{n/n_0})^p c^n$.

D'autre part, puisque T_1/T_0 est non ramifiée, l'idéal de T_0 engendré par w_0 est une puissance $n^{\text{ème}}$. Il s'en suit que w engendre dans T_0 un idéal qui est une puissance $n^{\text{ème}}$ (d'un idéal de T_0). Enfin, comme l'extension $T_0/\hat{K}_I$ est non ramifiée, l'idéal de $\hat{K}_I$ engendré par w est aussi la puissance $n^{\text{ème}}$ d'un idéal de $\hat{K}_I$.

Proposition 4. 2. *Pour toute puissance de l notée m et telle que $l \leq m \leq n$, on a :*

$$\dim_m W'/K_I^{*n} - \dim_m \mathcal{H}_I \leq \dim_l \mathcal{E}_I^0.$$

Démonstration. Soit A_{K_I} l'anneau des entiers de K_I . Soit w un élément de W' . D'après la proposition précédente il existe un idéal $\mathfrak{A}$ de K_I tel que $wA_{K_I} = \mathfrak{A}^n$. Comme l'idéal I' annule W'/K_I^{*n} (3. 4 et 3. 5), la classe de $\mathfrak{A}$ se trouve dans $\mathcal{H}_I$. En associant à wK_I^{*n} la classe de $\mathfrak{A}$, on définit un homomorphisme θ de W'/K_I^{*n} dans $\mathcal{H}_I$. On a donc la suite exacte

$$1 \rightarrow \text{Ker } \theta \rightarrow W'/K_I^{*n} \rightarrow \mathcal{H}_I$$

et l'application du lemme 2. 2 à cette suite fournit l'inégalité :

$$\dim_m W'/K_I^{*n} - \dim_m \mathcal{H}_I \leq \dim_l \text{Ker } \theta.$$

Examinons maintenant $\text{Ker } \theta$. Si la classe de w appartient à $\text{Ker } \theta$, il existe une unité ε de K_I telle que $w = \varepsilon a^n$. Cette unité vérifie les conditions suivantes: $L(\sqrt[n]{\varepsilon})/L$ est non ramifiée et ε^x appartient à K_I^{*n} pour tout x de I' . En associant à wK_I^{*n} la classe de ε modulo $E(K_I)^n$, on définit un homomorphisme de $\text{Ker } \theta$ dans $\mathcal{E}_I^0$. Cet homomorphisme est injectif, d'où la relation $\dim_l \text{Ker } \theta \leq \dim_l \mathcal{E}_I^0$.

Nous déduisons des lemmes 3. 2 et 3. 5 et de la proposition 4. 2 le théorème suivant :

Théorème 1'. *Soit m une puissance de l comprise entre l et n . On a l'inégalité :*

$$\dim_m \mathcal{H}^{\bar{I}} - \dim_m \mathcal{H}_I \leq \dim_l \mathcal{E}_I^0 + 1 \leq \dim_l \mathcal{E}_I + 1.$$

De plus, si $N \cap L = K_{\bar{I}}$, on a plus précisément :

$$\dim_m \mathcal{H}^{\bar{I}} - \dim_m \mathcal{H}_I \leq \dim_l \mathcal{E}_I^0 \leq \dim_l \mathcal{E}_I.$$

Le théorème 1, énoncé au paragraphe 1, s'en déduit, en utilisant le lemme suivant :

Lemme 4. 3. *Si l'une des hypothèses A_1 , B_1 , ou C_1 énoncées au paragraphe 1 est vérifiée, alors l'intersection $N \cap L$ est égale à $K_{\bar{I}}$.*

Démonstration. Le degré $[N:K_{\bar{I}}]$ est une puissance de l . Si A_1 est vérifiée, alors $[L:K_{\bar{I}}]$ est premier à $[N:K_{\bar{I}}]$ et $N \cap L = K_{\bar{I}}$. Supposons maintenant l'hypothèse B_1 vérifiée. Désignons par σ un générateur de $\text{Gal}(L/K_I)$. Comme $K_I^{(l)} \neq K_I$, nous aurons $\chi^*(\sigma) \not\equiv 1(l)$. D'autre part, puisque $\sigma - 1$ appartient à I , alors $\sigma - \chi^*(\sigma)$ appartient à $\bar{I}$. Soit u un générateur de $\text{Gal}(N \cap L/K_{\bar{I}})$. Faisons opérer $G_{\bar{I}}$ sur ce groupe par conjugaison. Désignons encore par σ la restriction de σ à $K_{\bar{I}}$. Comme L/k est abélienne, nous avons $u^\sigma = u$; par définition de N , on a $u^\sigma = u^{\chi^*(\sigma)}$, d'où $u^{\chi^*(\sigma)-1} = 1$ et $u = 1$. Si l'hypothèse C_1 est vérifiée, alors l'égalité $N \cap L = K_{\bar{I}}$ provient de la non ramification de l'extension $N/K_{\bar{I}}$.

5. Fin de la démonstration du théorème 2

Définition de W''' . Notons W''' l'ensemble des w de K_I^* vérifiant les trois conditions:

- 1) L'idéal engendré par w dans A_{K_I} est la puissance $n^{\text{ème}}$ d'un idéal de K_I .
- 2) Pour tout x de I' , w^x appartient à K_I^{*n} .
- 3) Pour tout idéal de K_I au-dessus de l , w est une puissance $n^{\text{ème}}$ dans le complété $\hat{K}_I$ de K_I pour cet idéal.

Il s'agit donc d'un groupe multiplicatif contenant K_I^{*n} . Le quotient W'''/K_I^{*n} est un $A_n[G_I]$ -module, annulé par I' . Pour tout w de W''' , nous notons $\langle w \rangle$ le sous-module de W'''/K_I^{*n} engendré par wK_I^{*n} et $L(\sqrt[n]{\langle w \rangle})/L$ l'extension de Kummer engendrée par les racines $n^{\text{èmes}}$ des éléments de $\langle w \rangle$. L'extension $L(\sqrt[n]{\langle w \rangle})/k$ est donc galoisienne. Il découle immédiatement de la définition de W''' , que $L(\sqrt[n]{\langle w \rangle})/L$ est non ramifiée. De plus, tout idéal de L au-dessus de l , y est totalement décomposé. D'autre part, l'idéal I annule $\langle w \rangle$. On déduit de la proposition 3. 3, que $\bar{I}$ annule $\text{Gal}(L(\sqrt[n]{\langle w \rangle})/L)$, considéré comme G -module.

On désigne par σ et $\tilde{\sigma}$ des générateurs de $\text{Gal}(L/K_I)$ et $\text{Gal}(L/K_{\bar{I}})$ respectivement. Pour tout u de $\text{Gal}(L(\sqrt[n]{\langle w \rangle})/L)$ on a $u^{\tilde{\sigma}} = u$ et, comme $\text{Gal}(L/K_{\bar{I}})$ est cyclique, il s'en suit que l'extension $L(\sqrt[n]{\langle w \rangle})/K_{\bar{I}}$ est abélienne. Nous allons maintenant montrer que, sous chacune des hypothèses A_1 , B_2 , B'_2 ou C_2 , le groupe W''' est inclus dans W' .

Proposition 5. 1. *Sous l'hypothèse A_1 (le degré de $L/K_{\bar{I}}$ est premier à l), le groupe W''' est inclus dans W' .*

Démonstration. Désignons par w un élément de W''' . Nous avons vu que le groupe $\text{Gal}(L(\sqrt[n]{\langle w \rangle})/K_{\bar{I}})$ est abélien. Il est donc produit direct de son l -sous-groupe de Sylow $\text{Gal}(L(\sqrt[n]{\langle w \rangle})/L)$ par un autre sous-groupe. Il existe donc un corps $N_{\langle w \rangle}$ tel que $L(\sqrt[n]{\langle w \rangle}) = N_{\langle w \rangle}L$ et $K_{\bar{I}} = N_{\langle w \rangle} \cap L$. L'extension $N_{\langle w \rangle}/K_{\bar{I}}$ est non ramifiée et de plus $N_{\langle w \rangle}/k$ est galoisienne: en effet, le groupe $\text{Gal}(L(\sqrt[n]{\langle w \rangle})/N_{\langle w \rangle})$ est le plus grand sous-groupe de $\text{Gal}(L(\sqrt[n]{\langle w \rangle})/K_{\bar{I}})$ d'ordre premier à l . Il est donc distingué dans $\text{Gal}(L(\sqrt[n]{\langle w \rangle})/k)$.

Puisque $\bar{I}$ annule le groupe $\text{Gal}(L(\sqrt[n]{\langle w \rangle})/L)$, alors par restriction, $\bar{I}'$ annule $\text{Gal}(N_{\langle w \rangle}/K_{\bar{I}})$. Ainsi, $N_{\langle w \rangle}$ est inclus dans N . Cela implique que $L(\sqrt[n]{\langle w \rangle})$ est inclus dans M , donc que w appartient à W' .

Proposition 5. 2. *Sous l'hypothèse C_2 (il existe un idéal premier et un seul de $K_{\bar{I}}$ qui est totalement ramifié dans $K_I^{(n)}/K_{\bar{I}}$), le groupe W''' est inclus dans W' .*

Démonstration. Nous désignons encore par w un élément de W''' . Nous définissons maintenant $N_{\langle w \rangle}$ comme le corps d'inertie dans $L(\sqrt[n]{\langle w \rangle})/K_{\bar{I}}$ de l'unique idéal ramifié de $L/K_{\bar{I}}$. On a donc $L(\sqrt[n]{\langle w \rangle}) = N_{\langle w \rangle} L$ et $K_{\bar{I}} = N_{\langle w \rangle} \cap L$. Si t appartient à $\text{Gal}(L(\sqrt[n]{\langle w \rangle})/k)$, alors notre idéal totalement ramifié est invariant par t (car il est le seul totalement ramifié) donc $N_{\langle w \rangle}$ est invariant par t , donc galoisien sur k . On conclut alors que $N_{\langle w \rangle}$ est inclus dans N , donc que w appartient à W' .

Lemme 5.3. *Supposons que l'hypothèse B_1 (le corps K_I ne contient pas de racine primitive $l^{\text{ème}}$ de 1) est vérifiée. Soit w un élément de W''' , alors il existe un corps $N_{\langle w \rangle}$ galoisien sur k , tel que $N_{\langle w \rangle} L = L(\sqrt[n]{\langle w \rangle})$ et $N_{\langle w \rangle} \cap L = K_{\bar{I}}$.*

Démonstration. Nous allons démontrer qu'il existe un unique corps $N_{\langle w \rangle}$, galoisien sur $K_I \cap K_{\bar{I}}$ et vérifiant les deux conditions $N_{\langle w \rangle} L = L(\sqrt[n]{\langle w \rangle})$ et $N_{\langle w \rangle} \cap L = K_{\bar{I}}$. De l'unicité résulte que $N_{\langle w \rangle}$ est galoisien sur k .

Introduisons s et $\tilde{s}$, prolongements respectifs de σ et $\tilde{\sigma}$ à $L(\sqrt[n]{\langle w \rangle})$ et posons $u = s^{-1} \tilde{s} s \tilde{s}^{-1}$. C'est un élément de $\text{Gal}(L(\sqrt[n]{\langle w \rangle})/L)$ et comme $\text{Gal}(L(\sqrt[n]{\langle w \rangle})/K_{\bar{I}})$ est abélien, on a $u \tilde{s} = \tilde{s} u$.

Pour tout entier β , $\tilde{s} u^\beta$ est encore un prolongement de $\tilde{\sigma}$ à $L(\sqrt[n]{\langle w \rangle})$. Montrons que l'on peut choisir β de façon que $\tilde{s} u^\beta$ vérifie l'égalité

$$s^{-1} (\tilde{s} u^\beta) s = \tilde{s} u^\beta$$

En effet $s^{-1} \tilde{s} u^\beta s = u \tilde{s} s^{-1} u^\beta s = \tilde{s} u^{\beta \chi^*(\sigma) + 1}$.

Compte-tenu de l'hypothèse B_1 , on a $\chi^*(\sigma) \not\equiv 1(l)$ et on peut choisir β de façon que $\beta(\chi^*(\sigma) - 1)$ soit congru à -1 , modulo l'ordre de u . Ainsi, nous avons trouvé un prolongement de $\tilde{\sigma}$, que l'on notera désormais $\tilde{s}$ et qui vérifie $s \tilde{s} = \tilde{s} s$.

On déduit de cette égalité que le sous-groupe engendré par $\tilde{s}$ est distingué dans $\text{Gal}(L(\sqrt[n]{\langle w \rangle})/(K_I \cap K_{\bar{I}}))$. Soit $N_{\langle w \rangle}$ le corps invariant par $\tilde{s}$. Il est galoisien sur $K_I \cap K_{\bar{I}}$ et il est clair que $N_{\langle w \rangle} \cap L$ est égal à $K_{\bar{I}}$. Montrons que $N_{\langle w \rangle} L = L(\sqrt[n]{\langle w \rangle})$. Si α est un entier et si $\tilde{s}^\alpha$ appartient à $\text{Gal}(L(\sqrt[n]{\langle w \rangle})/L)$ alors on aura d'une part $s^{-1} \tilde{s}^\alpha s = \tilde{s}^\alpha$, et d'autre part $s^{-1} \tilde{s}^\alpha s = (\tilde{s}^\alpha)^{\chi^*(\sigma)}$ car $\sigma - \chi^*(\sigma)$ appartient à $\bar{I}$ et annule $\text{Gal}(L(\sqrt[n]{\langle w \rangle})/L)$. Il s'en suit que $\tilde{s}^{\alpha(1 - \chi^*(\sigma))} = 1$ ce qui compte tenu de l'hypothèse B_1 , implique $\tilde{s}^\alpha = 1$. L'égalité cherchée en résulte.

Nous avons donc montré l'existence de $N_{\langle w \rangle}$ vérifiant les conditions annoncées. Il reste à démontrer l'unicité de $N_{\langle w \rangle}$. Supposons qu'il en existe un autre et notons S son composé avec $N_{\langle w \rangle}$. Le corps S est abélien sur $K_{\bar{I}}$ et l'action par conjugaison de s sur $\text{Gal}(S/K_{\bar{I}})$ est l'élevation à la puissance $\chi^*(\sigma)$. Compte tenu de l'hypothèse B_1 , on en déduit que $S \cap L = K_{\bar{I}}$. Mais alors le degré $[S:K_{\bar{I}}]$ est égal au produit $[L:K_{\bar{I}}][S:K_{\bar{I}}]$, ce qui implique l'inégalité $[S:K_{\bar{I}}] \leq [N_{\langle w \rangle}:K_{\bar{I}}]$; cette dernière est incompatible avec la définition de S et cela achève la démonstration.

Proposition 5. 4. *Si l'une ou l'autre des hypothèses:*

$B_2)$ le corps K_I ne contient pas de racine primitive $l^{\text{ème}}$ de 1 et il n'existe pas d'idéal au-dessus de l totalement décomposé dans $(K_I)_0/K_I \cap K_I$;

$B'_2)$ le corps K_I ne contient pas de racine primitive $l^{\text{ème}}$ de 1 et l'extension $K_I^{(n)}/K_I$ est modérément ramifiée;

est vérifiée, alors W''' est inclus dans W' .

Démonstration. Nous désignons encore par w un élément de W''' , et nous utilisons le lemme précédent. Si l'hypothèse B'_2 est vérifiée, alors $L(\sqrt[l]{\langle w \rangle})/K_I$ est modérément ramifiée en l , donc $N_{\langle w \rangle}/K_I$ est non ramifiée. Ainsi, $N_{\langle w \rangle}$ est inclus dans N donc w appartient à W' . Supposons maintenant l'hypothèse B_2 vérifiée. Choisissons un idéal de $L(\sqrt[l]{\langle w \rangle})$ au-dessus de l et pour désigner le localisé d'un corps relativement à cet idéal, surmontons le du signe $\hat{}$. On déduit de B_1 que $[\hat{K}_I : K_I \hat{\cap} K_I]$ n'est pas une puissance de l . Il existe donc τ dans le groupe de Galois de cette extension tel que $\chi^*(\tau) \not\equiv 1(l)$. Si u appartient à $\text{Gal}(\hat{N}_{\langle w \rangle}/\hat{K}_I)$, alors on a $u^\tau = u^{x^*(\tau)}$. D'autre part $u^\tau = u$ puisque, $\hat{L}$ étant égal à $\hat{L}(\sqrt[l]{w})$, le corps $\hat{N}_{\langle w \rangle}$ est inclus dans $\hat{L}$ donc est abélien sur $\hat{k}$.

On a donc $u^{x^*(\tau)-1} = 1$, d'où $u = 1$. Le corps $\hat{N}_{\langle w \rangle}$ est donc égal à $\hat{K}_I$ et tout idéal de K_I au-dessus de l est totalement décomposé dans $N_{\langle w \rangle}$. Finalement, l'extension $N_{\langle w \rangle}/K_I$ est non ramifiée, $N_{\langle w \rangle}$ est inclus dans N et w appartient à W' .

On déduit immédiatement de 5. 1, 5. 2 et 5. 4 la proposition suivante:

Proposition 5. 5. *Soit m une puissance de l , telle que $l \leq m \leq n$. Si l'une des hypothèses A_1 , B_2 , B'_2 ou C_2 est vérifiée, on a $\dim_m W'''/K_I^{*n} \leq \dim_m W'/K_I^{*n}$.*

Définitions de W'' , l_j , U_j , Π_j , $\mathcal{U}_{I(j)}$. On note W'' l'ensemble des w de K_I^* qui vérifient les deux conditions 1) et 2) introduites dans la définition de W''' , c'est-à-dire:

- 1) L'idéal de K_I engendré par w est une puissance $n^{\text{ème}}$ d'un idéal de K_I .
- 2) Pour tout x de I' , w^x appartient à K_I^{*n} .

Soient $l_1, l_2, \dots, l_t$ les idéaux de $K_I \cap K_I$ au-dessus de l . Choisissons, pour tout j de 1 à t , un idéal $\mathfrak{Q}_j$ de K_I au-dessus de l_j . Soit U_j le groupe des unités principales du complété de K_I en $\mathfrak{Q}_j$, soit Π_j une uniformisante de ce complété et soit D_j le groupe de décomposition de $\mathfrak{Q}_j$ dans K_I/k . Les groupes U_j/U_j^n sont des $A_n[D_j]$ -modules. Nous désignerons par $I(j)$ l'intersection de I' avec $A_n[D_j]$ et par $\mathcal{U}_{I(j)}$ le plus grand sous-module de U_j/U_j^n annulé par $I(j)$.

Nous pouvons maintenant énoncer

Proposition 5. 6. *Pour toute puissance de l , notée m et telle que $l \leq m \leq n$, on a l'inégalité:*

$$\dim_m W''/K_I^{*n} - \dim_m W'''/K_I^{*n} \leq \sum_{j=1}^t \dim_l \mathcal{U}_{I(j)}.$$

Démonstration. Soit w dans W'' et j entre 1 et t . L'idéal engendré par w étant une puissance $n^{\text{ème}}$, il existe p entier et u unité $\mathcal{O}_f$ -adique tels que l'on ait l'égalité $w = u \Pi_j^{np}$. Comme l'indice du groupe des unités principales U_j dans le groupe des unités $\mathcal{O}_f$ -adiques est premier à n , on peut écrire une relation de Bezout entre cet indice et n . On peut alors mettre u sous la forme $u' u''^n$ avec u' appartenant à U_j . Nous avons donc :

$$w = u' u''^n \Pi_j^{np}.$$

La quantité w étant définie modulo K_I^{*n} , u' est bien définie modulo U_j^n . Nous obtenons donc une application de W''/K_I^{*n} dans U_j/U_j^n en associant à $w K_I^{*n}$ la classe de u' modulo U_j^n . Cette application est un $A_n[D_j]$ -homomorphisme. Comme $I(j)$ annule W''/K_I^{*n} , l'image de cette application sera incluse dans $\mathcal{U}_{I(j)}$.

Si maintenant la quantité u' appartient à U_j^n , alors w sera une puissance $n^{\text{ème}}$ dans $\hat{K}_I$ localisé de K_I par l'idéal $\mathcal{O}_j$. Comme W''/K_I^{*n} est annulé par I et que $\tilde{\sigma} - \chi^*(\tilde{\sigma})$ appartient à I , alors $w^{\tilde{\sigma} - \chi^*(\tilde{\sigma})}$ appartient à K_I^{*n} . Ainsi, w sera aussi une puissance $n^{\text{ème}}$ dans les autres localisés de K_I pour les idéaux au-dessus de I_j .

Si l'hypothèse faite sur u' est réalisée pour tout j de 1 à t , alors w appartiendra à W''' . Nous avons donc montré que l'on peut construire une suite exacte :

$$1 \rightarrow W'''/K_I^{*n} \rightarrow W''/K_I^{*n} \rightarrow \bigoplus_{1 \leq j \leq t} \mathcal{U}_{I(j)}.$$

On déduit du lemme 2. 2, l'inégalité annoncée.

Définition de V , Λ et Λ_I . On note V l'ensemble des w de K_I qui vérifient la condition 1) introduite dans la définition de W''' c'est-à-dire :

- 1) L'idéal de K_I engendré par w est une puissance $n^{\text{ème}}$ d'un idéal de K_I .

Si w appartient à V , posons $w A_{K_I} = \mathfrak{A}^n$ et considérons l'homomorphisme Λ de V/K_I^{*n} dans $\mathcal{H}(K_I)^{(n)}$ qui associe à $w K_I^{*n}$ la classe de l'idéal $\mathfrak{A}$. C'est un homomorphisme surjectif de $A_n[G_I]$ -modules. Si $w K_I^{*n}$ appartient à W''/K_I^{*n} , alors son image par Λ appartient à $\mathcal{H}_I$. Nous désignons par Λ_I l'homomorphisme de W''/K_I^{*n} dans $\mathcal{H}_I$ qui associe à $w K_I^{*n}$ la classe de $\mathfrak{A}$. Son noyau est $[W'' \cap E(K_I) K_I^{*n}]/K_I^{*n}$, isomorphe à $\mathcal{E}_I$. On a donc une suite exacte :

$$1 \rightarrow \mathcal{E}_I \rightarrow W''/K_I^{*n} \rightarrow \mathcal{H}_I.$$

La proposition suivante est une conséquence du lemme 2. 3.

Proposition 5. 7. Soit m une puissance de l telle que $l \leq m \leq n$. Si Λ_I est surjectif, on a l'inégalité : $\dim_m \mathcal{H}_I \leq \dim_m W''/K_I^{*n}$. Si de plus $\mathcal{E}_I \cap \mathcal{E}(K_I)^m = \mathcal{E}_I^m$, on a plus précisément :

$$\dim_m \mathcal{H}_I + \dim_m \mathcal{E}_I \leq \dim_m W''/K_I^{*n}.$$

(Cette dernière condition est vérifiée au moins pour $m = n$ puisque $\mathcal{E}(K_I)^n = 1$.)

Proposition 5. 8. Soit m une puissance de l telle que $l \leq m \leq n$. Supposons que l'hypothèse A_2 introduite au paragraphe 1 (i.e. le degré de $[K_I : k]$ est premier à l et l'idéal I' de $A_n[G_I]$ est engendré par un idempotent) est vérifiée. Alors on a l'inégalité :

$$\dim_m \mathcal{H}_I + \dim_m \mathcal{E}_I \leq \dim_m W''/K_I^{*n}.$$

Démonstration. Nous formons à partir de l'application Λ la suite exacte:

$$1 \rightarrow E(K_I) K_I^{*n} / K_I^{*n} \rightarrow V / K_I^{*n} \rightarrow \mathcal{H}(K_I)^{(n)} \rightarrow 1.$$

Soit i l'idempotent de $A_n[G_I]$ engendrant l'idéal I' . Alors l'idéal engendré par $1-i$ est le supplémentaire de I' . On vérifie facilement que $[\mathcal{H}(K_I)^{(n)}]^{1-i}$ est égal à $\mathcal{H}_I$ et que $(V/K_I^{*n})^{1-i}$ est égal à W''/K_I^{*n} . Ainsi l'application Λ_I est encore surjective. Nous obtenons donc une suite exacte en élevant la précédente à la puissance $1-i$:

$$1 \rightarrow \mathcal{E}_I \rightarrow W''/K_I^{*n} \rightarrow \mathcal{H}_I \rightarrow 1.$$

Cette suite exacte vérifie, comme la précédente, la condition du lemme 2.3.

On trouvera au paragraphe 10, un autre cas particulier, où l'application Λ_I est surjective. Essayons de minorer maintenant la différence $\dim_m W''/K_I^{*n} - \dim_m \mathcal{H}_I$, en l'absence de cette hypothèse.

Définition de V'' . Soit V'' l'ensemble des éléments w de K_I vérifiant la condition 1) de la définition de W''' et une condition 2') plus faible que la condition 2) qui intervient dans la définition de W''' , à savoir:

- 1) L'idéal de K_I engendré par w est une puissance $n^{\text{ème}}$ d'un idéal de K_I .
- 2') Pour tout x de I' , w^x appartient à $K_I^{*n} E(K_I)$.

Le groupe V''/K_I^{*n} est un $A_n[G_I]$ -module mais il n'est pas annulé par I' . En associant à la classe de w appartenant à V'' , la classe de l'idéal $\mathfrak{A}$ tel que $wA_{K_I} = \mathfrak{A}^n$, on définit un homomorphisme surjectif de V''/K_I^{*n} dans $\mathcal{H}_I$ dont le noyau est $E(K_I) K_I^{*n} / K_I^{*n}$. Ce groupe est isomorphe à $\mathcal{E}(K_I)$. D'où la suite exacte:

$$1 \rightarrow \mathcal{E}(K_I) \rightarrow V''/K_I^{*n} \rightarrow \mathcal{H}_I \rightarrow 1.$$

Cette suite vérifie les conditions du lemme 2.3, nous en déduisons la proposition suivante:

Proposition 5.9. Soit m une puissance de l telle que $l \leq m \leq n$. On a l'inégalité:

$$\dim_m \mathcal{E}(K_I) + \dim_m \mathcal{H}_I \leq \dim_m V''/K_I^{*n}.$$

Essayons maintenant, pour terminer, de lier les m -rangs de V''/K_I^{*n} et W''/K_I^{*n} :

Proposition 5.10. Supposons que l'idéal I' de $A_n[G_I]$ puisse être engendré par s générateurs. Alors pour toute puissance de l , notée m et telle que $l \leq m \leq n$, on a:

$$\dim_m W''/K_I^{*n} \geq \dim_m V''/K_I^{*n} - s \dim_l \mathcal{E}(K_I).$$

Démonstration. Soit $\{x_1, \dots, x_s\}$ un système de générateurs de I' . Si w appartient à V'' , il existe, pour j de 1 à s , des unités ε_j et des éléments c_j de K_I tels que $w^{x_j} = \varepsilon_j c_j^n$. Les unités ε_j sont définies modulo $E(K_I)^n$. Associons à wK_I^{*n} la suite $(\varepsilon_j E(K_I)^n)_{1 \leq j \leq s}$. Nous définissons ainsi un homomorphisme de V''/K_I^{*n} dans $\bigoplus_{s \text{ copies}} \mathcal{E}(K_I)$ dont le noyau est W''/K_I^{*n} . Nous avons donc une suite exacte:

$$1 \rightarrow W''/K_I^{*n} \rightarrow V''/K_I^{*n} \rightarrow \bigoplus_{s \text{ copies}} \mathcal{E}(K_I).$$

Il suffit d'appliquer le lemme 2.2 à cette suite pour obtenir la relation annoncée.

Nous pouvons déduire des résultats de ce paragraphe et de l'inégalité $\dim_m W' \leq \dim_m \mathcal{H}^I$ démontrée au paragraphe 3, le théorème suivant:

Théorème 2'. Soit m une puissance de l telle que $l \leq m \leq n$. Si l'hypothèse suivante est vérifiée,

$A_2)$ le degré de $[K_I : k]$ est premier à l et l'idéal I' de $A_n[G_I]$ est engendré par un idempotent,

alors on a l'inégalité:

$$\dim_m \mathcal{E}_I - \sum_{j=1}^t \dim_l \mathcal{U}_{I(j)} \leq \dim_m \mathcal{H}^I - \dim_m \mathcal{H}_I.$$

Si l'une ou l'autre des hypothèses suivantes est vérifiée:

$B_2)$ le corps K_I ne contient pas de racine primitive $l^{\text{ème}}$ de 1 et il n'existe pas d'idéal au-dessus de I totalement décomposé dans $(K_I)_0 / K_I \cap K_I^-$,

$B'_2)$ le corps K_I ne contient pas de racine primitive $l^{\text{ème}}$ de 1 et l'extension $K_I^{(n)} / K_I^-$ est modérément ramifiée,

$C_2)$ il existe un idéal premier et un seul de K_I^- qui est totalement ramifié dans $K_I^{(n)} / K_I^-$,

alors on a l'inégalité:

$$- \sum_{j=1}^t \dim_l \mathcal{U}_{I(j)} - s \dim_l \mathcal{E}(K_I) + \dim_m \mathcal{E}(K_I) \leq \dim_m \mathcal{H}^I - \dim_m \mathcal{H}_I.$$

Si on suppose de plus que l'application A_I est surjective, on aura plus précisément:

$$- \sum_{j=1}^t \dim_l \mathcal{U}_{I(j)} \leq \dim_m \mathcal{H}^I - \dim_m \mathcal{H}_I$$

et même

$$\dim_m \mathcal{E}_I - \sum_{j=1}^t \dim_l \mathcal{U}_{I(j)} \leq \dim_m \mathcal{H}^I - \dim_m \mathcal{H}_I,$$

lorsque $\mathcal{E}_I \cap \mathcal{E}(K_I)^m = \mathcal{E}_I^m$ (cette dernière condition étant vérifiée, au moins pour $m = n$).

6. Majoration de $\dim_l \mathcal{E}_I$

Nous n'essons pas de majorer cette quantité dans le cas général. Nous nous limitons au cas où le corps de base k est le corps $\mathbb{Q}$ des rationnels. De plus lorsque l divise le degré de $K_I / \mathbb{Q}$, nous supposons que cette extension est cyclique. Pour alléger l'écriture nous modifions, pour ce paragraphe, les notations. Nous désignons par $K / \mathbb{Q}$ une extension abélienne finie qui, de plus, est cyclique lorsque l divise le degré de $K / \mathbb{Q}$ (cette extension joue le rôle de $K_I / \mathbb{Q}$), par H son groupe de Galois (remplaçant G_I), par J un idéal de $A_n[H]$ (remplaçant I'), par $E(K)$ le groupe des unités de K , par $\mathcal{E}(K)$ le quotient $E(K) / E(K)^n$ et par $\mathcal{E}_J$ l'ensemble des éléments de $\mathcal{E}(K)$ annulés par J . D'autre part, on note $\mathcal{E}'(K)$ le quotient $E(K) / E(K)^l$ et $\mathcal{E}'_J$ l'ensemble des éléments de $\mathcal{E}'(K)$ annulés par J . En général, si M est un $A_n[H]$ -module, on désigne par M_J le sous-module de M

formé des éléments annulés par J ; si M est un $\mathbb{F}_l[H]$ -module, c'est de manière canonique un $A_n[H]$ -module et M_J désigne encore l'ensemble des éléments de M annulés par J . On a donc $\mathcal{E}_J = \mathcal{E}(K)_J$ et $\mathcal{E}'_J = \mathcal{E}'(K)_J$.

A) *Le corps K est réel.* Dans ce cas l'élévation à la puissance n/l induit un isomorphisme de H -modules de $\mathcal{E}'(K)$ sur $\mathcal{E}(K)$. Tenant compte de l'égalité évidente $(\mathcal{E}(K)^{(l)})_J = (\mathcal{E}_J)^{(l)}$, on obtient $\dim_l \mathcal{E}_J = \dim_l \mathcal{E}'_J$; c'est cette dernière quantité que nous allons évaluer ici.

1°) *Le cas semi-simple* (i.e. $l \nmid [K:\mathbb{Q}]$). La structure du H -module $\mathcal{E}'(K)$ est alors donnée par le théorème de Dirichlet-Minkowsky (par ex. [12]). Le résultat peut s'énoncer sous la forme suivante:

Proposition 6. 1. *Si $v = \sum_{\tau \in H} \tau$, alors $\mathcal{E}'(K)$ est isomorphe en tant que $\mathbb{F}_l[H]$ -module à $\mathbb{F}_l[H]/v\mathbb{F}_l$. On a donc, pour tout idéal J , l'égalité $\dim_l \mathcal{E}_J = \dim_l (\mathbb{F}_l[H]/v\mathbb{F}_l)_J$.*

2°) *Le cas non semi-simple* (i.e. $l \mid [K:\mathbb{Q}]$). Comme nous l'avons indiqué plus haut, nous supposons ici que $K/\mathbb{Q}$ est cyclique. Nous posons $[K:\mathbb{Q}] = l^u d$ avec d premier à l et u supérieur ou égal à 1. Désignons par S , K_0 et T les sous-corps de K tels que $[K:S] = l$, $[K:K_0] = l^u$ et $[K:T] = d$. On note $E(S)$ le groupe des unités de S et $\mathcal{E}'(S)$ le quotient $E(S)/E(S)^l$.

L'intersection $E(K)^l \cap E(S)$ est réduite à $E(S)^l$: en effet si ε était un élément de $E(K)^l \cap E(S)$ n'appartenant pas à $E(S)^l$, les conjugués de ε par les éléments de $\text{Gal}(K/S)$ seraient les produits de ε par les racines $l^{\text{ièmes}}$ de l'unité; ces dernières appartiendraient donc au corps K ce qui est impossible puisque K est réel. On a donc la suite exacte:

$$1 \rightarrow \mathcal{E}'(S) \rightarrow \mathcal{E}'(K) \rightarrow E(K)/E(S) E(K)^l \rightarrow 1$$

d'où l'on tire la suite exacte plus courte

$$1 \rightarrow \mathcal{E}'(S)_J \rightarrow \mathcal{E}'_J \rightarrow (E(K)/E(S) E(K)^l)_J$$

(on rappelle que $\mathcal{E}'_J = \mathcal{E}'(K)_J$) dont nous allons étudier le dernier terme.

Lemme 6. 2. *Soit σ un élément d'ordre l de H (i.e. un générateur de $\text{Gal}(K/S)$). Alors le quotient $E(K)/E(S) E(K)^l$ est un $\mathbb{F}_l[H]$ -module isomorphe à $\mathbb{F}_l[H]/(1 + \sigma + \dots + \sigma^{l-1}) \mathbb{F}_l[H]$.*

Démonstration. Désignons par $E(K)$ et $E(S)$ les produits tensoriels $E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ et $E(S) \otimes_{\mathbb{Z}} \mathbb{Z}_l$; ce sont des $\mathbb{Z}_l[H]$ -modules. L'anneau $\mathbb{Z}_l$ étant $\mathbb{Z}$ -plat, $E(S)$ s'identifie à un sous module de $E(K)$ et le quotient $E(K)/E(S)$ que, pour alléger, nous noterons $E(K/S)$ est isomorphe à $(E(K)/E(S)) \otimes_{\mathbb{Z}} \mathbb{Z}_l$. On déduit de cela d'une part que $E(K/S)$ est sans $\mathbb{Z}_l$ -torsion (puisque $E(K)/E(S)$ est sans l -torsion) et d'autre part que $E(K)/E(S) E(K)^l$ est isomorphe à $E(K/S)/E(K/S)^l$. Notre lemme est donc conséquence du lemme suivant:

Lemme 6. 3. *On désigne toujours par σ un élément d'ordre l de H . Alors*

$$E(K/S) (= E(K)/E(S))$$

est un $\mathbb{Z}_l[H]$ -module isomorphe à $\mathbb{Z}_l[H]/(1 + \sigma + \dots + \sigma^{l-1}) \mathbb{Z}_l[H]$.

Démonstration. Soit $\bar{\mathbb{Q}}_l$ une clôture algébrique de $\mathbb{Q}_l$; pour tout groupe abélien G on note $\hat{G}$ le groupe des caractères l -adiques absolus de G i.e. le groupe des homomorphismes de G dans $\bar{\mathbb{Q}}_l^*$.

Si χ et χ' sont deux éléments de $\hat{G}$, on dit que χ est équivalent à χ' si il existe $\sigma \in \text{Gal}(\bar{\mathbb{Q}}_l/\mathbb{Q}_l)$ tel que $\chi = \sigma \cdot \chi'$. Le groupe G étant abélien, on a une correspondance bijective canonique entre les classes d'équivalences de $\hat{G}$ pour cette relation et les représentations l -adiques (i.e. rationnelles sur $\mathbb{Q}_l$) irréductible de G .

Le groupe H étant produit direct de ses sous groupes $\text{Gal}(K/K_0)$ et $\text{Gal}(K/T)$, le groupe $\hat{H}$ s'identifie canoniquement au produit $\widehat{\text{Gal}(K/K_0)} \times \widehat{\text{Gal}(K/T)}$. Pour tout $i=0, \dots, u$ désignons par $\chi_0^{(i)}$ un homomorphisme de $\text{Gal}(K/K_0)$ dans $\bar{\mathbb{Q}}_l^*$ dont le noyau est d'ordre l^{u-i} ; il est clair que les $\chi_0^{(i)}$ décrivent un système complet de représentants des classes de $\widehat{\text{Gal}(K/K_0)}$. D'autre part, désignons par $\chi_T^{(j)}$ pour $j=0, \dots, r-1$ un système complet de représentants des classes de $\widehat{\text{Gal}(K/T)}$. Pour tout couple (i, j) où $i=0, \dots, u$ et $j=0, \dots, r-1$ on note $\chi_{i,j}$ l'élément de $\hat{H}$ correspondant au couple $(\chi_0^{(i)}, \chi_T^{(j)})$ de $\widehat{\text{Gal}(K/K_0)} \times \widehat{\text{Gal}(K/T)}$; les $\chi_{i,j}$ décrivent un système de représentants de $\hat{H}$. On note respectivement $M_{i,j}$ et $1_{i,j}$ le module simple et l'idempotent de la représentation l -adique attachée à $\chi_{i,j}$. Le théorème de Minkowski-Dirichlet ([12] par exemple) montre que le $\mathbb{Q}_l[H]$ -module $E(K) \otimes_{\mathbb{Q}_l} \mathbb{Q}_l$ est isomorphe à la somme directe $\bigoplus_{(i,j)} M_{i,j}$ où i varie de 0 à u , j varie de 0 à $r-1$ et où $(i, j) \neq (0, 0)$.

Considérons maintenant le groupe $\text{Gal}(S/\mathbb{Q}) = H/\text{Gal}(K/S)$. Le groupe $\widehat{\text{Gal}(S/\mathbb{Q})}$ s'identifie avec les éléments de $\hat{H}$ qui sont triviaux sur $\text{Gal}(K/S)$; modulo cette identification, il est clair que les $\chi_{i,j}$ pour $i \neq u$ et j quelconque forment un système de représentants des classes d'équivalence de $\widehat{\text{Gal}(S/\mathbb{Q})}$. Le $\mathbb{Q}_l[\text{Gal}(S/\mathbb{Q})]$ -module simple de la représentation l -adique irréductible de $\text{Gal}(S/\mathbb{Q})$ associée à l'un de ces $\chi_{i,j}$ est canoniquement muni d'une structure de $\mathbb{Q}_l[H]$ -module et est alors isomorphe à $M_{i,j}$. On déduit donc, de nouveau du théorème de Minkowski-Dirichlet, que le $\mathbb{Q}_l[H]$ -module $E(S) \otimes_{\mathbb{Q}_l} \mathbb{Q}_l$ est isomorphe à $\bigoplus_{(i,j)} M_{i,j}$ où i varie de 0 à $u-1$, j varie de 0 à $r-1$ et où $(i, j) \neq (0, 0)$.

D'autre part, $\mathbb{Q}_l$ étant $\mathbb{Z}_l$ -plat, on a

$$(E(k) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l) / (E(S) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l) = E(K/S) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l;$$

on déduit donc de ce qui précède que $E(K/S) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l = \bigoplus_{j=0}^{r-1} M_{u,j}$.

Rappelons que, si $\zeta_{u,j}$ est l'image par $\chi_{u,j}$ d'un générateur de H , alors $\chi_{u,j}$ se prolonge par linéarité en une surjection d'anneaux de $\mathbb{Q}_l[H]$ sur $\mathbb{Q}_l(\zeta_{u,j})$; on munit ainsi $\mathbb{Q}_l(\zeta_{u,j})$ d'une structure de $\mathbb{Q}_l[H]$ -module et ce $\mathbb{Q}_l[H]$ -module est isomorphe à $M_{u,j}$.

Considérons maintenant le groupe $\text{Gal}(K/T)$. Ses représentations irréductibles sont canoniquement associées aux classes d'équivalence des caractères absolument irréductibles $\chi_T^{(0)}, \dots, \chi_T^{(r-1)}$; notons $e_0, \dots, e_{r-1}$ les idempotents de $\mathbb{Q}_l[\text{Gal}(K/T)]$ associés à ces représentations. L'ordre de $\text{Gal}(K/T)$ étant premier à l , ces idempotents sont dans

$\mathbb{Z}_l[\text{Gal}(K/T)]$ donc aussi dans $\mathbb{Z}_l[H]$. Ils permettent donc de décomposer canoniquement les $\mathbb{Z}_l[H]$ -modules. Enfin on vérifie que, pour tout j , on a (dans $Q_l[H]$) l'égalité $e_j = \sum_{i=0}^u 1_{i,j}$. Le $\mathbb{Z}_l[H]$ -module $E(K/S)$ est égal à $\prod_{j=0}^{r-1} E(K/S)^{e_j}$. On a donc $E(K/S) \otimes_{\mathbb{Z}_l} Q_l = \prod_{j=0}^{r-1} (E(K/S)^{e_j} \otimes_{\mathbb{Z}_l} Q_l)$. Remplaçons e_j par $\sum_{i=0}^u 1_{i,j}$; d'autre part $E(K/S)^{e_j} \otimes_{\mathbb{Z}_l} Q_l = (E(K/S) \otimes_{\mathbb{Z}_l} Q_l)^{1_{u,j}}$ puisque $e_j = \sum_{i=0}^u 1_{i,j}$ et que $(E(K/S) \otimes_{\mathbb{Z}_l} Q_l)^{1_{i,j}}$ est nul si $i \neq u$.

De plus, $E(K/S)$ étant sans $\mathbb{Z}_l$ -torsion, il s'injecte dans $E(K/S) \otimes_{\mathbb{Z}_l} Q_l$; en conséquence $E(K/S)^{e_j}$ s'injecte dans $(E(K/S) \otimes_{\mathbb{Z}_l} Q_l)^{1_{u,j}}$. Ce dernier module étant, comme nous l'avons vu ci-dessus, isomorphe au $Q_l[H]$ -module $Q_l(\zeta_{u,j})$, l'action d'un élément de $Q_l[H]$ sur lui ne dépend que de l'image de cet élément par $\chi_{u,j}$. Il en résulte que l'action d'un élément de $\mathbb{Z}_l[H]$ sur $E(K/S)^{e_j}$ ne dépend que de l'image de cet élément par $\chi_{u,j}$. Cet image est l'anneau $\mathbb{Z}_l[\zeta_{u,j}]$, donc $E(K/S)^{e_j}$ est un $\mathbb{Z}_l[\zeta_{u,j}]$ -module; montrons qu'il est isomorphe à $\mathbb{Z}_l[\zeta_{u,j}]$. On a déjà vu qu'il est sans $\mathbb{Z}_l$ -torsion; de plus son produit tensoriel par Q_l sur $\mathbb{Z}_l$ est $(E(K/S) \otimes_{\mathbb{Z}_l} Q_l)^{1_{u,j}}$ qui est isomorphe à $Q_l(\zeta_{u,j})$; son $\mathbb{Z}_l$ -rang est donc égal au degré de $Q_l(\zeta_{u,j})/Q_l$ donc est le $\mathbb{Z}_l$ -rang de $\mathbb{Z}_l[\zeta_{u,j}]$. En conséquence le $\mathbb{Z}_l[\zeta_{u,j}]$ -module $E(K/S)^{e_j}$ est monogène; le morphisme $\chi_{u,j}$ envoyant surjectivement $e_j \mathbb{Z}_l[H]$ sur $\mathbb{Z}_l[\zeta_{u,j}]$, le $e_j \mathbb{Z}_l[H]$ -module $E(K/S)^{e_j}$ est monogène. On en déduit que

$$\prod_{j=0}^{r-1} E(K/S)^{e_j} = E(K/S) \text{ est un module monogène sur } \bigoplus_{j=0}^{r-1} e_j \mathbb{Z}_l[H] = \mathbb{Z}_l[H],$$

i.e. qu'il y a une surjection de $\mathbb{Z}_l[H]$ -module de $\mathbb{Z}_l[H]$ sur $E(K/S)$. Enfin $E(K/S)$ étant annulé par $1 + \sigma + \dots + \sigma^{l-1}$, on en déduit une surjection de $\mathbb{Z}_l[H]$ -modules de $\mathbb{Z}_l[H]/(1 + \sigma + \dots + \sigma^{l-1}) \mathbb{Z}_l[H]$ sur $E(K/S)$; ces deux modules sans $\mathbb{Z}_l$ -torsion ayant le même rang, cette surjection est un isomorphisme, ce qui achève la démonstration.

Introduisons maintenant pour i variant de 0 à u , le sous-corps K_i de K tel que $[K : K_i] = l^{u-i}$ et H_i le groupe de Galois de K_i/Q . (On a donc $K_u = K$ et $H_u = H$.)

Proposition 6. 4. *Pour i variant de 1 à u , soit σ_i un élément d'ordre l de H_i . Soit $M_i = \mathbb{F}_l[H_i]/(1 + \sigma_i + \dots + \sigma_i^{l-1}) \mathbb{F}_l[H_i]$. C'est un $\mathbb{F}_l[H]$ -module. Soit d'autre part $M_0 = \mathbb{F}_l[H_0]/v \mathbb{F}_l$, avec $v = \sum_{\tau \in H_0} \tau$. Alors, (K/Q étant cyclique et réelle) on a:*

$$\dim_l(M_0)_J \leq \dim_l \mathcal{E}_J \leq \dim_l(M_0)_J + \sum_{i=1}^u \dim_l(M_i)_J.$$

Dans le cas particulier, où J est principal, alors on a plus simplement:

$$\dim_l \mathcal{E}_J \leq \dim_l(M_0)_J + u \dim_l(M_u)_J.$$

Démonstration. Soit $\mathcal{E}'(K_i) = E(K_i)/E(K_i)^I$. On déduit de la suite exacte écrite au début de ce paragraphe et du lemme 6.2 l'inégalité:

$$\dim_l \mathcal{E}'(K_u)_J \leq \dim_l \mathcal{E}'(K_{u-1})_J + \dim_l (M_u)_J.$$

Une récurrence évidente et la proposition 6.1 donnent le résultat.

Si J est principal, les inégalités $\dim_l (M_i)_J \leq \dim_l (M_u)_J$ résultent du lemme suivant:

Lemme 6.5. *Soit B un $\mathbb{F}_l$ -espace vectoriel de dimension finie, A un sous-espace de B et α un endomorphisme de B tel que $\alpha(A)$ soit inclus dans A . Cet endomorphisme induit par passage au quotient un endomorphisme α' de B/A . Alors les dimensions des noyaux sont liées par:*

$$\dim_l \text{Ker } \alpha' \leq \dim_l \text{Ker } \alpha.$$

Appliquons ce lemme à $B = M_u$. On peut déduire de l'homomorphisme de restriction de H_u sur H_{u-1} , un homomorphisme surjectif de M_u sur M_{u-1} . Prenons pour A le noyau de cet homomorphisme et pour α la multiplication par le générateur de J . On obtient l'inégalité: $\dim_l (M_{u-1})_J \leq \dim_l (M_u)_J$.

B) *Cas imaginaire.* Nous supposons maintenant que l'extension $K/\mathbb{Q}$ est imaginaire. Notons σ_∞ la conjugaison complexe de H . Nous supposons aussi que $\sigma_\infty + 1$ appartient à l'idéal J .

Remarque 6.6. Cette hypothèse est vérifiée dès que K est le corps K_I , correspondant dans l'involution définie au paragraphe 1, à un corps $K_{\bar{I}}$ réel.

En effet, reprenons un instant les notations du paragraphe 1: Supposons que k soit égal à $\mathbb{Q}$ et que $K_{\bar{I}}$ soit réel. Alors la conjugaison complexe de G , notée encore σ_∞ , appartient à $\text{Ker } \bar{I}$ et $\sigma_\infty - 1$ appartient à $\bar{I}$. Comme $\chi^*(\sigma_\infty) = -1$, la quantité $\sigma_\infty + 1$ appartient à I .

Si K contient une racine primitive $l^{\text{ème}}$ de 1, ζ_l , nous notons encore χ^* l'application de H dans $\mathbb{F}_l^*$ définie par $\zeta_l^\tau = \zeta_l^{\chi^*(\tau)}$ pour tout τ de H . Nous définissons alors $\mathbb{F}_l^{\chi^*}$ comme le $\mathbb{F}_l[H]$ -module de support $\mathbb{F}_l$ sur lequel un τ de H agit comme la multiplication par $\chi^*(\tau)$ (ce module est donc isomorphe au module multiplicatif engendré par ζ_l).

Proposition 6.7. *Le corps K étant imaginaire, on suppose que l'idéal J contient $\sigma_\infty + 1$. Si K ne contient pas de racine primitive $l^{\text{ème}}$ de 1, on a $\dim_l \mathcal{E}_J = 0$. Si K contient une racine primitive $l^{\text{ème}}$ de 1, alors on a:*

$$\dim_l \mathcal{E}_J = \dim_l (\mathbb{F}_l^{\chi^*})_J \leq 1.$$

Démonstration. Le groupe $\mathcal{E}(K)$ se décompose en produit direct

$$\mathcal{E}(K) = \mathcal{E}(K)^{(1+\sigma_\infty)/2} \mathcal{E}(K)^{(1-\sigma_\infty)/2}.$$

Comme $\sigma_\infty + 1$ appartient à J , on en déduit immédiatement $(\mathcal{E}(K)^{(1+\sigma_\infty)/2})_J = 1$. D'autre part, si K_0 est le sous-corps réel maximal de K , l'injection canonique de $E(K_0)$ dans $E(K)$ induit un isomorphisme de $\mathcal{E}(K_0)$ sur $\mathcal{E}(K)^{(1+\sigma_\infty)/2}$. Il résulte du théorème de Dirichlet, que $\mathcal{E}(K)^{(1-\sigma_\infty)/2}$ est réduit à 1 si K ne contient pas de racine primitive $l^{\text{ème}}$ de 1. Sinon $\mathcal{E}(K)^{(1-\sigma_\infty)/2}$ est cyclique, engendré par une racine de 1.

7. Majoration de $\dim_l \mathcal{U}_{I(J)}$

Nous essayons dans ce paragraphe d'appliquer quelques résultats concernant la structure du groupe des unités d'un corps local à la majoration de $\dim_l \mathcal{U}_{I(J)}$. Comme au paragraphe précédent, nous ne donnerons des résultats que sous certaines hypothèses; par exemple le complété l -adique du corps de base k est égal à $\mathbb{Q}_l$.

Dans ce paragraphe, nous désignons par:

$K/\mathbb{Q}_l$ une extension abélienne, D son groupe de Galois,

J un idéal de $A_n[D]$,

U le groupe des unités principales de K ,

$\mathcal{U}(K) = U/U^n$ et $\mathcal{U}_J$ l'ensemble des éléments de $\mathcal{U}(K)$ annihilés par J .

Comme au paragraphe précédent, on notera M_J l'ensemble des éléments du $A_n[D]$ -module M annihilés par J .

Si K contient une racine primitive $l^{\text{ème}}$ de 1, disons ζ_l , on désignera encore par χ^* l'application de D dans $\mathbb{F}_l^*$ définie par

$$\zeta_l^{\chi^*(\tau)} = \zeta_l^\tau.$$

On notera $\mathbb{F}_l^{\chi^*}$ le $\mathbb{F}_l[D]$ -module de support $\mathbb{F}_l$ sur lequel un τ de D opère par multiplication par $\chi^*(\tau)$ et $\mathbb{F}_l^\tau$ le $\mathbb{F}_l[D]$ -module de support $\mathbb{F}_l$ sur lequel D opère trivialement.

On déduit de [7] ou de [13] (théorème 2. 5):

Proposition 7. 1. *Si $K/\mathbb{Q}_l$ est modérément ramifiée et ne contient pas de racine primitive $l^{\text{ème}}$ de 1, $\mathcal{U}(K)^{(l)}$ est isomorphe à $\mathbb{F}_l[D]$. On a donc:*

$$\dim_l \mathcal{U}_J = \dim_l \mathbb{F}_l[D]_J.$$

On déduit de [5] ou de [13], (théorème 20):

Proposition 7. 2. *On suppose que $K/\mathbb{Q}_l$ est modérément ramifiée et contient une racine primitive $l^{\text{ème}}$ de 1. Si $n = l$, alors $\mathcal{U}(K)$ est isomorphe à $\mathbb{F}_l^{\chi^*} \oplus \mathbb{F}_l[D]$ et on a donc:*

$$\dim_l \mathcal{U}_J = \dim_l (\mathbb{F}_l^{\chi^*})_J + \dim_l \mathbb{F}_l[D]_J.$$

Posons $\varrho = \sum_{\tau \in D} \chi^*(\tau^{-1})\tau$. Si $n \geq l^2$, alors $\mathcal{U}(K)$ est isomorphe à

$$\mathbb{F}_l^{\chi^*} \oplus \mathbb{F}_l^{\chi^*} \oplus \mathbb{F}_l[D]/\varrho \mathbb{F}_l[D].$$

Et on a donc:

$$\dim_l \mathcal{U}_J = 2 \dim_l (\mathbb{F}_l^{\chi^*})_J + \dim_l (\mathbb{F}_l[D]/\varrho \mathbb{F}_l[D])_J.$$

Remarque 7. 3. Dans le cas particulier où le degré $[K:\mathbb{Q}_l]$ est premier à l , alors $\varrho \mathbb{F}_l[D]$ est facteur direct dans $\mathbb{F}_l[D]$ et isomorphe à $\mathbb{F}_l^{\chi^*}$. Il s'en suit que l'on a toujours dans ce cas:

$$\dim_l \mathcal{U}_J = \dim_l (\mathbb{F}_l^{\chi^*})_J + \dim_l \mathbb{F}_l[D]_J.$$

Proposition 7. 4. *On suppose que K/Q_l est cyclique et que K ne contient pas de racine primitive $l^{\text{ème}}$ de 1. Soit $v = \sum_{\tau \in D} \tau$. On a :*

$$\dim_l \mathcal{U}_J \leq \dim_l (F_l^v)_J + \dim_l (F_l[D]/vF_l)_J.$$

La démonstration s'appuie sur les résultats de [1] : Puisque K ne contient pas de racine primitive $l^{\text{ème}}$ de 1, alors $\mathcal{U}(K)^{(l)}$ est isomorphe à U/U^l . Soit N l'application norme dans K/Q_l . On déduit de la suite exacte :

$$1 \rightarrow \text{Ker } N \rightarrow U \rightarrow N(U) \rightarrow 1,$$

la suite exacte :

$$1 \rightarrow \text{Ker } N/(\text{Ker } N)^l \rightarrow U/U^l \rightarrow N(U)/N(U)^l \rightarrow 1.$$

Le dernier terme est isomorphe à F_l^v . Quant au quotient $\text{Ker } N/(\text{Ker } N)^l$, on déduit de [1] théorème 1, qu'il est isomorphe à $F_l[D]/vF_l$. D'où le résultat annoncé.

Nous ne connaissons pas de résultat permettant de majorer $\dim_l \mathcal{U}_J$ dans le cas plus général où K/Q_l serait sauvagement ramifiée et contiendrait des racines $l^{\text{èmes}}$ de 1. (Voir toutefois, pour les corps cyclotomiques [6].)

8. Le «Spiegelungssatz» de Leopoldt [9]

Voyons tout d'abord que le théorème 1 contient le «Spiegelungssatz». Supposons donc que le degré $[L:k]$ est premier à l (hypothèse faite par Leopoldt). Soit Φ un caractère l -adique de G irréductible. Soit 1_Φ l'idempotent associé. Il est donné par :

$$1_\Phi = \frac{1}{[L:k]} \sum_{\tau \in G} \Phi(\tau^{-1}) \tau.$$

C'est un élément de l'algèbre $\mathbb{Z}_l[G]$. Considérons l'idéal I de $A_n[G]$ engendré par le résidu modulo n de $1 - 1_\Phi$. Soit $\mathcal{H}(L)$ le l -groupe des classes d'idéaux de L . Le groupe des classes d'idéaux considéré en [9] est $\mathcal{H}(L)^{1_\Phi}$. On vérifie immédiatement que l'injection canonique de $\mathcal{H}(K_l)$ dans $\mathcal{H}(L)$ induit un isomorphisme de $\mathcal{H}^l$ sur $\mathcal{H}(L)^{1_\Phi}/[\mathcal{H}(L)^{1_\Phi}]^n$. On a donc l'égalité $\dim_m \mathcal{H}^l = \dim_m \mathcal{H}(L)^{1_\Phi}$, pour toute puissance de l , notée m et telle que $l \leq m \leq n$. On vérifie aussi que $\mathcal{H}_I$ est isomorphe à $[\mathcal{H}(L)^{(n)}]^{1_\Phi}$; on a donc aussi $\dim_m \mathcal{H}_I = \dim_m \mathcal{H}(L)^{1_\Phi}$.

L'application χ^* de G dans A_n^* est, sous l'hypothèse $l \nmid [L:k]$, le résidu d'un homomorphisme de G dans $\mathbb{Z}_l^*$ que l'on note encore χ^* . Leopoldt définit une involution sur les caractères l -adiques irréductibles de G , en posant $\bar{\Phi} = \chi^* \Phi^{-1}$. L'idéal que nous avons noté $\bar{I}$ est évidemment engendré par le résidu modulo n de l'idempotent $1 - 1_{\bar{\Phi}}$.

Soit $E(L)$ le groupe des unités de L et $E^0(L)$ le groupe des unités l -primaires de L . On vérifie aussi que :

$$\dim_l (E(L)/E(L)^l)^{1_\Phi} = \dim_l \mathcal{E}_I \quad \text{et} \quad \dim_l (E^0(L)/E(L)^l)^{1_\Phi} = \dim_l \mathcal{E}_I^0.$$

On déduit alors du théorème 1 les inégalités :

$$\dim_{\mathcal{H}} \mathcal{H}(L)^{1\bar{\Phi}} - \dim_{\mathcal{H}} \mathcal{H}(L)^{1\Phi} \leq \dim_l (E^0(L)/E(L)^l)^{1\Phi} \leq \dim_l (E(L)/E(L)^l)^{1\Phi},$$

qui sont celles démontrées dans [9].

9. Cas particulier où l'idéal I' est engendré par un polynôme cyclotomique

Nous allons montrer que l'on peut, sans l'hypothèse restrictive du paragraphe précédent, associer à un caractère l -adique de G un idéal de $A_n[G]$.

Soit donc Φ un caractère l -adique irréductible de G et 1_Φ son idempotent. Nous notons I_0 l'idéal de $\mathbb{Z}_l[G]$ formé des x de $\mathbb{Z}_l[G]$ tels que $x \cdot 1_\Phi = 0$. Nous définissons alors I comme l'image de I_0 par la surjection canonique de $\mathbb{Z}_l[G]$ sur $A_n[G]$. D'autre part, on désigne par I'_0 l'image de I_0 par la surjection canonique de $\mathbb{Z}_l[G]$ dans $\mathbb{Z}_l[G_l]$ et I' est toujours l'image de I dans $A_n[G_l]$. Choisissons un caractère absolument irréductible χ au-dessus de Φ . On peut préciser la correspondance entre Φ et I de la manière suivante :

Proposition 9. 1. *Le noyau de χ coïncide avec le noyau de I , donc l'extension K_I/k est cyclique. Soit σ un générateur de G_I et $P_{\sigma, \Phi}(Y)$ le polynôme cyclotomique l -adique ayant $\chi(\sigma)$ pour racine, alors l'idéal I'_0 est engendré par $P_{\sigma, \Phi}(\sigma)$; l'idéal I' est donc principal et engendré par le résidu modulo n de $P_{\sigma, \Phi}(\sigma)$.*

Nous ne démontrons pas cette proposition.

Remarque 9. 2. Les groupes $\mathcal{H}_I$ et $\mathcal{E}_I$ attachés à un idéal I de $A_n[G]$ provenant d'un caractère l -adique Φ sont à rapprocher des Φ -objets introduits par G. Gras dans [3].

Remarque 9. 3. Si I est un idéal de $A_n[G]$ obtenu à partir d'un caractère l -adique, il ne semble pas que, l'idéal $\bar{I}$ puisse en général être obtenu de cette manière. On peut voir cependant que c'est le cas si le corps de base k contient le corps $\mathbb{Q}_l^{(n)}$ défini par $[\mathbb{Q}^{(n)} : \mathbb{Q}_l^{(n)}] = l - 1$. En effet, dans ce cas χ^* est le résidu modulo n d'un caractère χ^{**} l -adique de G . En posant (comme en [9]), $\bar{\Phi} = \Phi^{-1} \chi^{**}$, on définit un autre caractère l -adique irréductible $\bar{\Phi}$ de G et l'idéal $\bar{I}$ lui est associé.

10. Cas particulier des pseudo-caractères de degré 1

Par définition, un pseudo-caractère de degré 1 est un homomorphisme de G dans A_n^* . A tout pseudo-caractère ψ de degré 1, on associe un idéal I de $A_n[G]$ de la manière suivante: on prolonge ψ par linéarité en un homomorphisme d'anneaux ψ_1 de $A_n[G]$ vers A_n et I est le noyau de ψ_1 . On montre alors sans difficulté que le noyau de l'idéal I coïncide avec le noyau de ψ . Il en résulte que l'extension K_I/k est cyclique; nous notons σ un générateur de son groupe de Galois G_I et φ l'homomorphisme de G_I dans A_n^* déduit de ψ par passage au quotient. On établit facilement la proposition suivante :

Proposition 10. 1. *L'image I' de I dans $A_n[G_l]$ est l'idéal principal engendré par $\sigma - \varphi(\sigma)$. De plus, si $\bar{\psi} = \chi^* \psi^{-1}$, l'idéal $\bar{I}$ est l'idéal associé au pseudo-caractère $\bar{\psi}$.*

Remarque 10. 2. L'homomorphisme φ de G_I dans A_n^* est injectif. Réciproquement, si l'on se donne une extension K/k cyclique (jouant le rôle de K_I/k), σ un générateur de son groupe de Galois et φ un homomorphisme injectif de ce groupe de Galois dans A_n^* , alors l'idéal principal de $A_n[\text{Gal}(K/k)]$ engendré par $\sigma - \varphi(\sigma)$ a un noyau trivial; on peut donc le prendre comme idéal I' , c'est le point de vue adopté par Ph. Satgé dans [14].

Le lemme suivant montre que, dans le cas des pseudo-caractères, l'entier t intervenant dans le théorème 2 est égal à 1.

Lemme 10. 3. *On suppose que le corps de base est $\mathbb{Q}$ et que I est associé à un pseudo-caractère. Alors l'intersection $K_I \cap K_I^-$ est contenu dans $\mathbb{Q}^{(n)}$.*

Démonstration. Soit ψ le pseudo-caractère définissant I . Soit $\bar{\psi}$ le produit $\psi^{-1}\chi^*$; compte tenu de la proposition 10.1, notre lemme est équivalent à l'inclusion $(\text{Ker } \psi) \cdot (\text{Ker } \bar{\psi}) \supset \text{Ker } \chi^*$. Pour démontrer cette inclusion, remarquons que l'hypothèse $k = \mathbb{Q}$ implique la surjectivité de l'homomorphisme χ^* de G dans A_n^* , donc de $\psi\bar{\psi}$. Choisissons un générateur a de A_n^* et choisissons un σ_0 de G tel que $\psi\bar{\psi}(\sigma_0) = a$. Définissons h et $\bar{h}$ par les égalités $\psi(\sigma_0) = a^h$ et $\bar{\psi}(\sigma_0) = a^{\bar{h}}$; on a $h + \bar{h} \equiv 1 \pmod{n}$ puisque $\psi\bar{\psi}(\sigma_0) = a$. Soit maintenant σ dans $\text{Ker } \chi^*$; définissons r et $\bar{r}$ par $\psi(\sigma) = a^r$ et $\bar{\psi}(\sigma) = a^{\bar{r}}$; on a $r + \bar{r} \equiv 0 \pmod{n}$ puisque $(\psi\bar{\psi})(\sigma) = \chi^*(\sigma) = 1$. On a donc $\sigma = (\sigma^h \sigma_0^{-r})(\sigma^{\bar{h}} \sigma_0^{-\bar{r}})$ qui montre que σ est dans $(\text{Ker } \psi)(\text{Ker } \bar{\psi})$ et achève la démonstration.

Revenons à l'application Λ_I définie au paragraphe 5. On a la proposition suivante:

Proposition 10. 4. *Si l'idéal I est associé à un pseudo-caractère, si $k = \mathbb{Q}$ et si K_I ne contient pas de racine de l'unité d'ordre l , alors l'homomorphisme Λ_I est surjectif.*

Nous aurons besoin du lemme suivant que nous énonçons sans démonstration:

Lemme 10. 5. *Soit f un entier d'ordre d modulo n , il existe f' tel que $f \equiv f' \pmod{n}$ et que $f'^d \not\equiv 1 \pmod{nl}$.*

Démonstration (de la proposition 10.4). Soit $d = [K_I : \mathbb{Q}]$ et soit f un entier dont la classe modulo n est $\varphi(\sigma)$ et qui est tel que $f^d \not\equiv 1 \pmod{nl}$. Désignons par y le P.G.C.D de n et de $1 + f + \dots + f^{d-1}$, et par λ le quotient $(1 + f + \dots + f^{d-1})/y$; ce nombre λ est premier à l .

Soit maintenant $\mathfrak{A}$ un idéal de K_I dont la classe $\text{Cl}(\mathfrak{A})$ est dans $\mathcal{H}_I$. Il existe a et b dans K_I tels que $aA_{K_I} = \mathfrak{A}^n$ et $\mathfrak{A}^{\sigma^{-f}} = bA_{K_I}$. Il existe donc une unité ε de K_I telle que $a^{\sigma^{-f}} = b^n \varepsilon$. Une récurrence simple montre alors que $a^{\sigma^j} = a^{f^j} \varepsilon^{x_{j-1}} b_j^n$, avec

$$x_{j-1} = f^{j-1} + f^{j-2} \sigma + \dots + f \sigma^{j-2} + \sigma^{j-1} \text{ et } b_j \text{ dans } K_I.$$

En multipliant terme à terme ces égalités (pour j allant de 0 à $d-1$) et en remarquant que la norme de a dans K_I/Q est une puissance $n^{\text{ième}}$, on voit que $a^{1+f+\dots+f^{d-1}} \varepsilon^{x_0+\dots+x_{d-2}}$ est une puissance $n^{\text{ième}}$ dans K_I . De l'égalité $1+f+\dots+f^{d-1}=\lambda y$, on déduit qu'il existe une unité ε_0 de K_I telle que

$$\varepsilon_0^{-y} = \varepsilon^{x_0+\dots+x_{d-2}}.$$

Un calcul simple montre alors que

$$\varepsilon_0^{-y(\sigma-f)} = \varepsilon^{1+f+\dots+f^{d-1}}$$

et, K_I ne contenant pas de racine de l'unité d'ordre l , il en résulte que $\varepsilon_0^{\sigma-f} = \varepsilon^\lambda$. Comme λ est premier à l , on en déduit l'existence d'unités ε_1 et ε_2 de K_I telles que

$$\varepsilon_1^{\sigma-f} \varepsilon_2^n = \varepsilon.$$

On termine la démonstration en vérifiant que $a\varepsilon_1^{-1}$ appartient à W'' et a pour image $\text{Cl}(\mathfrak{A})$ par l'homomorphisme A_I .

Terminons ce paragraphe en explicitant les inégalités des théorèmes 1' et 2' dans la situation particulière des idéaux associés aux pseudo-caractères. L'entier l intervenant dans le théorème 2' étant égal à 1, on écrit $\mathcal{U}_I$ à la place de $\mathcal{U}_{I(1)}$; de plus la proposition 10.5 permet d'employer la forme forte du théorème 2'; enfin, pour le type d'idéaux considéré ici, les résultats des paragraphes 6 et 7 permettent de calculer explicitement les invariants $\dim_l \mathcal{U}_I$ et $\dim_l \mathcal{E}_I$ au moins lorsque les complétés de K_I au dessus de l ne contiennent pas de racine de l'unité d'ordre l . On obtient ainsi la proposition suivante:

Proposition 10.6. *On suppose que I est associé à un pseudo-caractère de degré 1. On suppose aussi que $k=Q$ et que l'hypothèse B_2 est vérifiée. On a alors les inégalités*

$$\dim_l \mathcal{E}_I - \dim_l \mathcal{U}_I \leq \dim_n \mathcal{H}^{\bar{I}} - \dim_n \mathcal{H}_I \leq \dim_l \mathcal{E}_I.$$

De plus, on a $\dim_l \mathcal{U}_I = 1$ ou 2 et $\dim_l \mathcal{E}_I = 0$ si K_I est imaginaire.

Si K_I est réel et si l^u est la plus grande puissance de l qui divise le degré de K_I/k , on a $1 \leq \dim_l \mathcal{E}_I \leq u+1$.

11. Exemple des corps cyclotomiques

Pour ne pas compliquer les notations, nous nous limiterons à $Q^{(l^2)}$. Dans ce paragraphe nous posons $n=l^2$, $L=Q^{(n)}$, $k=Q$, $G=\text{Gal}(L/Q)$ et $\chi=\chi^*$. Nous désignons par $Q_1^{(n)}$ le sous-corps de $Q^{(n)}$ tel que $[Q^{(n)}/Q_1^{(n)}]=l-1$ et H le groupe de Galois $\text{Gal}(Q^{(n)}/Q_1^{(n)})$.

Essayons d'abord d'appliquer à ce cas particulier le Spiegelungssatz de Leopoldt [9], c'est-à-dire le théorème 1 sous l'hypothèse A_1 . Nous ne pouvons pas, dans ce cadre, choisir un corps de base plus petit que $Q_1^{(n)}$. Choisissons donc $Q_1^{(n)}$ et désignons par Φ la restriction de χ à H . Les résidus modulo n des caractères l -adiques irréductibles de H sont $\bar{\Phi}, \bar{\Phi}^2, \dots, \bar{\Phi}^{l-1}$. Le caractère miroir χ^* est dans ce cas $\bar{\Phi}$ et l'involution $\bar{\Phi}^i \rightarrow \bar{\Phi}^i$ est définie par $\bar{\Phi}^i = \bar{\Phi}^{1-i}$. Introduisons l'idempotent $1_{\bar{\Phi}^i}$ associé à $\bar{\Phi}^i$ et $\mathcal{H}_{\bar{\Phi}^i}$ le groupe des classes $\mathcal{H}(L)^{1_{\bar{\Phi}^i}}$. On tire de [9] (ou du théorème 1) la proposition:

Proposition 11.1. *Supposons que i soit un entier pair tel que $i \not\equiv 0 \pmod{l-1}$. Alors, pour $m=l$ et l^2 , les m -rangs de $\mathcal{H}_{\bar{\Phi}^i}$ et $\mathcal{H}_{\bar{\Phi}^{1-i}}$ sont liés par:*

$$0 \leq \dim_m \mathcal{H}_{\bar{\Phi}^{1-i}} - \dim_m \mathcal{H}_{\bar{\Phi}^i} \leq l.$$

Le point de vue développé dans les théorèmes 1 et 2 permet de tenir compte de l'action du groupe G tout entier sur les classes d'idéaux. Pour cela nous prenons $\mathbb{Q}$ comme corps de base. Les puissances de χ sont les pseudo-caractères de degré 1 de G . Choisissons un entier j et notons I l'idéal associé à χ^j (par la méthode du paragraphe 10); dans la suite on pose $K_{\chi^j} = K_I$, $\mathcal{H}_{\chi^j} = \mathcal{H}_I$ et $\mathcal{H}^{\chi^j} = \mathcal{H}^I$.

Examinons d'abord quel rapport il y a entre ces groupes et les groupes $\mathcal{H}_{\Phi^i}$ précédents. Désignons par K_{Φ^i} le corps intermédiaire entre $\mathbb{Q}^{(n)}$ et $\mathbb{Q}_1^{(n)}$ tel que $\text{Ker } \Phi^i = \text{Gal}(L/K_{\Phi^i})$. Le groupe de classes d'idéaux $\mathcal{H}_{\Phi^i}$ peut être considéré comme un sous-groupe du groupe $\mathcal{H}(K_{\Phi^i})$ des l -classes d'idéaux de K_{Φ^i} . Il est alors facile de vérifier que si j est un entier tel que $j \not\equiv 0 \pmod{l}$, K_{χ^j} coïncide avec K_{Φ^j} , le groupe $\mathcal{H}_{\chi^j}$ est un sous-groupe de $\mathcal{H}_{\Phi^j}$ et le groupe $\mathcal{H}^{\chi^j}$ est un quotient de $\mathcal{H}_{\Phi^j}$. On a donc les relations:

$$\dim_m \mathcal{H}^{\chi^j} \leq \dim_m \mathcal{H}_{\Phi^j}$$

et

$$\dim_m \mathcal{H}_{\chi^j} \leq \dim_m \mathcal{H}_{\Phi^j}, \quad \text{pour } m = l \text{ et } l^2.$$

On déduit des théorèmes 1' et 2' que les l^2 -rangs des groupes $\mathcal{H}_{\chi^j}$ et $\mathcal{H}^{\chi^j}$ vérifient des inégalités plus contraignantes que les précédentes. On a:

Proposition 11. 2. *Soit j un entier tel que $j \not\equiv 0 \pmod{l-1}$ et $j \not\equiv 0 \pmod{l}$. Alors on a:*

$$\begin{aligned} 0 &\leq \dim_n \mathcal{H}^{\chi^{1-j}} - \dim_n \mathcal{H}_{\chi^j} \leq 2 \quad \text{si } j \text{ est pair} \\ -1 &\leq \dim_n \mathcal{H}^{\chi^{1-j}} - \dim_n \mathcal{H}_{\chi^j} \leq 0 \quad \text{si } j \text{ est impair.} \end{aligned}$$

Démonstration. Les inégalités de droite proviennent du théorème 1' (sous l'hypothèse C') et de la proposition 6. 4. Pour démontrer les inégalités de gauche, distinguons trois cas:

Supposons d'abord que j soit pair. Alors K_{χ^j} est un sous-corps réel de $\mathbb{Q}^{(n)}$. Donc il ne contient pas de racine $l^{\text{ème}}$ de 1 et son complété l -adique non plus. Notons $\mathcal{U}_I$ au lieu de $\mathcal{U}_{I(1)}$ (car dans ce cas, il est clair que t vaut 1). On déduit de la proposition 7. 4 l'inégalité $\dim_l \mathcal{U}_I \leq 1$. Mais on peut aussi appliquer la proposition 10. 6 et la différence des n -rangs de $\mathcal{H}^{\chi^{1-j}}$ et $\mathcal{H}_{\chi^j}$ est minorée par 0.

Supposons maintenant que j soit impair et non premier à $l-1$. Alors, dans ce cas le corps K_{χ^j} est imaginaire, mais différent de $\mathbb{Q}^{(n)}$. Son complété l -adique ne contiendra pas non plus de racine primitive $l^{\text{ème}}$ de 1 et on majore $\dim_l \mathcal{U}_I$ comme précédemment.

Supposons enfin que j soit premier à $l-1$. Alors, dans ce cas le corps K_{χ^j} est égal à $\mathbb{Q}^{(n)}$. Les résultats énoncés dans le paragraphe 7 ne permettent plus de majorer $\dim_l \mathcal{U}_I$. Mais on trouve dans [6] un résultat de structure des groupes d'unités des corps cyclotomiques l -adiques qui permet de conclure que $\dim_l \mathcal{U}_I$ est majoré comme précédemment par 1.

Bibliographie

- [1] Z. I. Borevič, The multiplicative group of a regular local field with a cyclic group of operators, (En russe), Izvetzia Akad. Nauk SSSR, Ser. Mat. **28** (1964), 707—712.
- [2] C. Chevalley, Sur deux théorèmes d'Arithmétique, J. Math. Soc. Japan **3** (1951).
- [3] G. Gras, Application de la notion de φ -objet à l'étude du groupe des classes d'idéaux des extensions abéliennes, Publ. Math. Fac. Sciences Besançon, 1975—1976.
- [4] H. Hasse, Invariante Kennzeichnung relativ abelscher Zahlkörper mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers, Abh. Deutsche Akad. Wiss. Berlin 1947.
- [5] K. Iwasawa, On Galois groups of local fields, Trans. Amer. Math. Soc. **80** (1955), 448—469.
- [6] K. Iwasawa, On local cyclotomic fields, J. Math. Soc. Japan, **12** (1960).
- [7] M. Krasner, Sur la représentation exponentielle dans les corps relativement galoisiens de nombres p -adiques, Acta Arith. **3** (1939), 133—173.
- [8] S. Lang, Algebra, Reading, Mass. 1969.
- [9] H. W. Leopoldt, Zur Struktur der l -Klassengruppe galoisscher Zahlkörper, J. reine angew. Math. **199** (1958).
- [10] B. Oriat, Relations entre les 2-groupes des classes d'idéaux des extensions quadratiques $k(\sqrt{d})$ et $k(\sqrt{-d})$, Ann. l'Institut Fourier **27** (1977).
- [11] B. Oriat, Relation entre les 2-groupes des classes d'idéaux au sens ordinaire et restreint de certains corps de nombres, Bull. Soc. Math. France **104** (1976).
- [12] B. Oriat, Spiegelungssatz, Publ. Math. Fac. Sciences Besançon, 1975—1976.
- [13] H. Pieper, Die Einheitengruppe eines zahm-verzweigten galoisschen lokalen Körpers als Galois-Modul, Math. Nachr. **54** (1972), 173—210.
- [14] P. Satgé, Inégalités de miroir, Séminaire Delange-Pisot-Poitou: Théorie des Nombres, 18ème Année, 1976/1977, n° 18.
- [15] A. Scholtz, Über die Beziehung der Klassenzahlen quadratischer Körper zueinander, J. reine angew. Math. **166** (1931), 201—203.

Mathématiques, ERA N° 070654, Faculté des Sciences, F-25030 Besançon Cedex
 Mathématiques, Faculté des Sciences, F-14032 Caen Cedex

Eingegangen 30. Mai 1978

GENERALISATION DU "SPIEGELUNGSSATZ"

par

Bernard Oriat

La propriété qui nous intéresse ici est celle énoncée par Leopoldt dans [3]. Nous la rappelons dans les paragraphes I et II. Dans le paragraphe III nous montrons comment nous avons essayé d'en obtenir une généralisation. Dans le dernier paragraphe un principe analogue est appliqué pour déduire du théorème de Stickelberger une propriété d'annulation de classes d'idéaux réelles.

I Spiegelungsrelation.

Soit L/k une extension galoisienne finie de corps de nombres, de groupe de Galois G . On suppose que L contient toutes les racines $n^{\text{ème}}$ de 1. Soit M/L une extension abélienne d'exposant divisant n . C'est une extension de Kummer ; désignons par W son radical, c'est-à-dire l'ensemble des w de L tels que $\sqrt[n]{w}$ appartienne à M . On suppose que W est stable par G , c'est-à-dire que M/k est galoisienne. Le groupe G opère, en tant que groupe de Galois, sur W , donc sur W/L^{*n} . D'autre part on peut le faire opérer par conjugaison sur $\text{Gal}(M/L)$. Ainsi les deux groupes W/L^{*n} et $\text{Gal}(M/L)$ sont des $(\mathbb{Z}/n\mathbb{Z})[G]$ modules.

D'autre part, soit ζ_n une racine primitive $n^{\text{ème}}$ de 1 et $\langle \zeta_n \rangle$ le groupe multiplicatif qu'elle engendre. On définit un homomorphisme χ^* de G dans $(\mathbb{Z}/n\mathbb{Z})^*$ par l'égalité :

$$\zeta_n^\sigma = \zeta_n^{\chi^*(\sigma)}, \text{ pour tout } \sigma \text{ de } G.$$

Les deux groupes W/L^{*n} et $\text{Hom}(\text{Gal}(M/L), \langle \zeta_n \rangle)$, groupe dual de $\text{Gal}(M/L)$, sont canoniquement isomorphes. Si α est l'isomorphisme en question, rappelons qu'il est défini par : $\alpha(wL^{*n})(u) = w^{u-1}$, pour tout u de $\text{Gal}(M/L)$. Nous pouvons maintenant énoncer la "Spiegelungsrelation" [3] :

Théorème : Pour tout w de W , tout τ de G et tout u de $\text{Gal}(M/L)$, on a

B. ORLAT

l'égalité :

$$\alpha((wL^{*n})^\tau)(u) = \alpha(wL^{*n})(u^{X^*(\tau)} \tau^{-1}).$$

Définition de l'involution du miroir. On peut définir dans l'algèbre de groupe $(\mathbb{Z}/n\mathbb{Z})[G]$ une involution en faisant correspondre à $x = \sum_{\tau \in G} a_\tau \tau$,

l'élément $\bar{x} = \sum_{\tau \in G} a_\tau X^*(\tau) \tau^{-1}$. Nous l'appelons : involution du miroir. Si

G est abélien, il s'agit d'un automorphisme de $(\mathbb{Z}/n\mathbb{Z})[G]$. La "Spiegelungsrelation" peut s'écrire à l'aide de cette involution sous la forme :

$$\alpha((wL^{*n})^x)(u) = \alpha(wL^{*n})(u^{\bar{x}});$$

pour tout w de W , tout u de $\text{Gal}(M/L)$ et tout x de $(\mathbb{Z}/n\mathbb{Z})[G]$.

Utilisation de la "Spiegelungsrelation" : Dans la suite, la situation décrite ci-dessus est utilisée de la façon suivante : L'extension M/L est non ramifiée. Son groupe de Galois est donc, par la théorie du corps de classes, isomorphe en tant que G -module, à un groupe quotient du groupe des classes de L . Si w appartient à W , alors l'idéal de L qu'il engendre est une puissance $n^{\text{ème}}$ d'un idéal $\mathfrak{a}$ de L . En associant à w la classe de l'idéal $\mathfrak{a}$, on définit une application de W/L^{*n} dans le groupe des classes de L . Le noyau de cet homomorphisme s'exprime alors à l'aide d'un groupe d'unités de L . On dispose ainsi d'un moyen de comparer un quotient du groupe des classes d'idéaux de L (ou d'un sous-corps de L) à un sous-groupe du groupe des classes de L (ou d'un sous-corps de L). De plus, si x annule le premier groupe, alors $\bar{x}$ annule le deuxième.

II Le "Spiegelungssatz" de Leopoldt [3].

Soit ℓ un nombre premier. Dans ce paragraphe on prend $n = \ell$ et on pose l'hypothèse suivante : ℓ ne divise pas le degré $[L : k]$.

Soit ψ un caractère ℓ -adique de G et $1_\psi = \frac{1}{[L : k]} \sum_{\tau \in G} \psi(\tau) \tau^{-1}$

l'idempotent de $\mathbb{Q}_\ell[G]$ associé. Il y a une correspondance biunivoque entre les idempotents de $\mathbb{Q}_\ell[G]$ et les idempotents de $\mathbb{F}_\ell[G]$ déduite de l'application canonique de $\mathbb{Z}_\ell[G]$ sur $\mathbb{F}_\ell[G]$. Si on confond un idempotent avec son résidu modulo ℓ , on voit que l'image $\bar{1}_\psi$ de 1_ψ par l'involution du miroir est un idempotent associé à un caractère $\bar{\psi}$ de G . Ce caractère $\bar{\psi}$ peut être défini de la façon suivante : Soit θ l'unique homomorphisme de G dans $\mathbb{Z}_\ell^*$

"SPIEGELUNGSSATZ"

défini par $\zeta_\ell^\tau = \zeta_\ell^{\theta(\tau)}$ pour tout τ de G . On a alors $\bar{\psi} = \theta\psi^{-1}$ et l'application $\psi \rightarrow \bar{\psi}$ est une involution de l'ensemble des caractères ℓ -adiques de G .

Soit $\mathcal{K}(L)$ le ℓ -groupe des classes de L . A chaque caractère ψ , on associe le groupe $\mathcal{K}(L)^\psi$. Le "Spiegelungssatz" compare les ℓ -rangs (notés $\dim_\ell$) des groupes $\mathcal{K}(L)^\psi$ et $\mathcal{K}(L)^{\bar{\psi}}$. Introduisons encore $E(L)$ groupe des unités de L et $\mathcal{E}(L) = E(L)/E(L)^\ell$.

Théorème : Si ℓ ne divise pas $[L : k]$ et si ψ est un caractère ℓ -adique de G , alors on a l'inégalité :

$$\dim_\ell \mathcal{K}(L)^\psi - \dim_\ell \mathcal{K}(L)^{\bar{\psi}} \leq \dim_\ell \mathcal{E}(L)^{\bar{\psi}}.$$

III Généralisation du Spiegelungssatz [4].

Dans cette généralisation on ne fait plus l'hypothèse : ℓ ne divise pas $[L : k]$, posée dans [3]. Les idempotents 1_ψ ne sont plus des éléments entiers et la notation $\mathcal{K}(L)^\psi$ n'a plus de sens. Soit maintenant ℓ un nombre premier impair. On désigne par n une puissance de ℓ . L'extension L/k est supposée abélienne de groupe de Galois G . On suppose toujours que L contient toutes les racines $n^{\text{ème}}$ de 1.

Les groupes d'idéaux et d'unités considérés sont attachés maintenant, non plus à un caractère ℓ -adique du groupe G , mais à un idéal I de l'algèbre $(\mathbb{Z}/n\mathbb{Z})[G]$. Définissons le corps K_I comme le corps intermédiaire entre L et k tel que $\text{Gal}(L/K_I) = \{\sigma; \sigma \in G; \sigma-1 \in I\}$. Si $\mathcal{K}(K_I)$ est le ℓ -groupe des classes d'idéaux de K_I , le groupe $\mathcal{K}_I$ est défini comme le plus grand quotient de $\mathcal{K}(K_I)/\mathcal{K}(K_I)^n$ annulé par I . De même, si $\mathcal{K}(K_I)^{(n)}$ est le sous-groupe de $\mathcal{K}(K_I)$ formé des éléments h de $\mathcal{K}(K_I)$ tels que $h^n = 1$, $\mathcal{K}_I$ est défini comme le plus grand sous-groupe de $\mathcal{K}(K_I)^{(n)}$ annulé par I .

Remarque : Ces définitions généralisent la définition précédente : en effet si ℓ ne divise pas $[L : k]$ et si ψ est un caractère ℓ -adique de G , soit I l'idéal de $(\mathbb{Z}/n\mathbb{Z})[G]$ engendré par $1-\psi$. Alors on vérifie que les groupes $\mathcal{K}_I$, $\mathcal{K}_I$ et $\mathcal{K}_I^\psi$ ont même ℓ -rang.

De la même façon, désignons par $E(K_I)$ le groupe des unités de K_I , $\mathcal{E}(K_I)$ le quotient $E(K_I)/E(K_I)^n$ et $\mathcal{E}_I$ le plus grand sous-groupe de

B. ORLAT

$\mathcal{E}(K_1)$ annulé par 1. Précisons enfin que $\bar{I}$ désigne l'image de I par l'involution du miroir et que $\dim_m$ désigne le m -rang.

Théorème. Pour toute puissance de ℓ , notée m et comprise entre ℓ et n , on a l'inégalité :

$$\dim_m \mathcal{X}^I - \dim_m \mathcal{X}_{\bar{I}} \leq \dim_{\ell} \mathcal{E}_{\bar{I}} + 1.$$

De plus, si l'une ou l'autre des hypothèses suivantes est vérifiée :

- Le degré $[L : K_1]$ est premier à ℓ ,
- Le corps $K_{\bar{I}}$ ne contient pas de racine primitive $\ell^{\text{ème}}$ de 1 ; alors

on a plus précisément :

$$\dim_m \mathcal{X}^I - \dim_m \mathcal{X}_{\bar{I}} \leq \dim_{\ell} \mathcal{E}_{\bar{I}}.$$

Remarquons que le changement de I en $\bar{I}$ ne permute pas $\mathcal{X}^I$ et $\mathcal{X}_{\bar{I}}$. Ainsi, obtenir une minoration de la différence $\dim_m \mathcal{X}^I - \dim_m \mathcal{X}_{\bar{I}}$ est, dans ce cadre plus général, un autre problème. Pour énoncer l'un des résultats obtenus, introduisons un groupe d'unités locales : Soient $\ell_1, \dots, \ell_t$ les idéaux de $K_1 \cap K_{\bar{I}}$ au-dessus de ℓ et D_j le groupe de décomposition de ℓ_j dans l'extension L/k . Soit $\bar{I}(j) = (\mathbb{Z}/n\mathbb{Z})[D_j] \cap \bar{I}$ et U_j le groupe des unités principales du complété de $K_{\bar{I}}$ en un idéal au-dessus de ℓ_j . Soit $\mathcal{U}_{\bar{I}(j)}$ le plus grand sous-module de U_j/U_j^n annulé par $\bar{I}(j)$. Soit s le nombre de générateurs de l'image de l'idéal $\bar{I}$ par l'application restriction de $(\mathbb{Z}/n\mathbb{Z})[G]$ à $(\mathbb{Z}/n\mathbb{Z})[\text{Gal}(K_{\bar{I}}/k)]$. Désignons par $(K_1)_0$ le corps intermédiaire entre K_1 et $K_1 \cap K_{\bar{I}}$, maximal tel que $[(K_1)_0 : K_1 \cap K_{\bar{I}}]$ soit premier à ℓ .

Théorème. Si aucun idéal, au-dessus de ℓ , n'est totalement décomposé dans $(K_1)_0/K_1 \cap K_{\bar{I}}$ et si $K_{\bar{I}}$ ne contient pas de racine primitive $\ell^{\text{ème}}$ de 1, alors, on a :

$$- \sum_{j=1}^t \dim_{\ell} \mathcal{U}_{\bar{I}(j)} - (s-1) \dim_{\ell} \mathcal{E}(K_{\bar{I}}) \leq \dim_m \mathcal{X}^I - \dim_m \mathcal{X}_{\bar{I}},$$

pour toute puissance de ℓ , notée m et comprise entre ℓ et n .

On trouvera dans [4] d'autres inégalités minorant la différence $\dim_m \mathcal{X}^I - \dim_m \mathcal{X}_{\bar{I}}$, valables sous d'autres hypothèses. Mais, en l'absence d'hypothèse, nous ne savons pas minorer cette différence.

IV Annulation de classes d'idéaux réelles.

Nous désignons toujours par ℓ un nombre premier impair. Soit

"SPIEGELUNGSSATZ"

χ un caractère réel de conducteur f et ψ le caractère ℓ -adique issu de χ . Notons $\mathbb{Q}_\ell^{(\chi)}$ le corps obtenu en adjoignant à $\mathbb{Q}_\ell$ les valeurs prises par χ et $\mathbb{Z}_\ell^{(\chi)}$ l'anneau des entiers de ce corps. On associe à ψ un groupe de classes d'idéaux de la façon suivante :

Soit K_χ le sous-corps de $\mathbb{Q}^{(f)}$ tel que $\text{Gal}(\mathbb{Q}^{(f)}/K_\chi)$ soit égal à $\text{Ker } \chi$. (Le caractère χ étant considéré comme un homomorphisme de $\text{Gal}(\mathbb{Q}^{(f)}/\mathbb{Q})$ dans $\mathbb{Q}_\ell^{(\chi)*}$). Soit $G = \text{Gal}(K_\chi/\mathbb{Q})$. On peut encore considérer χ comme un homomorphisme de G dans $\mathbb{Q}_\ell^{(\chi)*}$. Nous notons χ_1 son prolongement $\mathbb{Z}_\ell$ -linéaire à $\mathbb{Z}_\ell[G]$. C'est un homomorphisme d'anneaux, de $\mathbb{Z}_\ell[G]$ dans $\mathbb{Z}_\ell^{(\chi)}$ et il est surjectif. Si on considère ψ comme un caractère de G et si 1_ψ est l'idempotent de $\mathbb{Q}_\ell[G]$ associé à ψ , le noyau de χ_1 est égal à $\mathbb{Z}_\ell[G] \cap (1 - 1_\psi) \mathbb{Q}_\ell[G]$. Si $\mathcal{K}(K_\chi)$ est le ℓ -groupe des classes de K_χ , notons $\mathcal{K}^\psi$ le plus grand quotient de $\mathcal{K}(K_\chi)$ annulé par le noyau de χ_1 . Ainsi $\mathcal{K}^\psi$ est un module sur $\mathbb{Z}_\ell^{(\chi)}$.

Le résultat suivant est démontré par G. Gras dans [2] :

Théorème : Si ℓ est un nombre premier impair, si χ est un caractère réel différent de 1 et si ℓ ne divise pas l'ordre de χ , alors $\mathcal{K}^\psi$ est, en tant que $\mathbb{Z}_\ell^{(\chi)}$ -module, annulé par $L_\ell(1, \chi)$, valeur en 1 de la fonction L ℓ -adique relative à χ .

Remarque : En fait, le résultat obtenu en [2] est plus précis : Il concerne un groupe de classes généralisées, correspondant par la théorie du corps de classes à une extension non ramifiée, sauf en ℓ , de K_χ .

Nous avons démontré que l'hypothèse " ℓ ne divise pas l'ordre de χ " peut être remplacée par l'hypothèse : "l'ordre de χ n'est pas une puissance de ℓ ".

La démonstration de cette propriété utilise toujours les mêmes principes : en voici le résumé : Décomposons le conducteur f de χ sous la forme $f = f_0 n_0$ avec f_0 premier à ℓ et n_0 puissance de ℓ . Soit n une puissance de ℓ , supérieure à n_0 . On désigne par L_n le corps obtenu en ajoutant à K_χ toutes les racines $n^{\text{ème}}$ de 1 et on pose $G_n = \text{Gal}(L_n/\mathbb{Q})$. On introduit l'extension non ramifiée, M_n/L_n , qui correspond par le corps de classes au groupe de classes $\mathcal{K}^\psi/(\mathcal{K}^\psi)^n$ et on construit comme indiqué au paragraphe I, un homomorphisme de $\mathcal{K}^\psi/(\mathcal{K}^\psi)^n$ dans le ℓ -groupe des

B. ORIAT

classes de L_n . (Les corps M_n , L_n , Q correspondent à M , L et k). Comme K_X est réel, cet homomorphisme est injectif. Le groupe des classes de L_n est annulé par l'idéal de Stickelberger de L_n . On en déduit que l'image par l'involution du miroir (de L_n/Q) de l'idéal de Stickelberger annule le groupe $X_\Psi / (X_\Psi)^n$.

Désignons par $(\frac{L_n}{\cdot})$ le symbole d'Artin attaché à L_n et choisissons un entier a_0 premier à f_0 et à ℓ , tel que $\chi(a_0)$ ne soit pas une racine de 1 d'ordre une puissance de ℓ . Introduisons les éléments suivants de l'algèbre $Q_\ell[G_n]$:

$$x_n = \frac{1}{f_0 n \varphi(n)} \left[1 - \left(\frac{L_n}{a_0} \right) a_0^{\varphi(n)} \right] \sum_{\substack{1 \leq a \leq f_0 n \\ (a, f_0 n) = 1}} a^{\varphi(n)} \left(\frac{L_n}{a} \right)$$

$$\text{et } y_n = \frac{1}{f_0 n} \left[1 - \left(\frac{L_n}{a_0} \right)^{-1} a_0 \right] \sum_{\substack{1 \leq a \leq f_0 n \\ (a, f_0 n) = 1}} a \left(\frac{L_n}{a} \right)^{-1},$$

où φ désigne l'indicateur d'Euler. On vérifie facilement qu'il s'agit d'éléments de $Z_\ell[G_n]$ et la démonstration de la proposition suivante est élémentaire :

Proposition. Les résidus modulo n de x_n et y_n sont des éléments de $(Z/nZ)[G_n]$, images l'un de l'autre par l'involution du miroir attachée à l'extension L_n/Q .

Mais y_n appartient à l'idéal de Stickelberger de L_n et on en déduit donc que x_n annule $X_\Psi / (X_\Psi)^n$. Si maintenant on cherche l'image de x_n par χ_1 , on voit que cet élément va s'écrire sous la forme d'un produit :

$$\chi_1(x_n) = \left[1 - \chi(a_0) a_0^{\varphi(n)} \right] \left[\frac{1}{f_0 n \varphi(n)} \sum_{\substack{1 \leq a \leq f_0 n \\ (a, f_0 n) = 1}} a^{\varphi(n)} \chi(a) \right]$$

dont le premier terme est une unité de $Z_\ell^{(\chi)}$. On reconnaît dans le deuxième l'approximation ℓ -adique de $L_\ell(1, \chi)$ telle qu'elle est donnée dans [1]. Il

"SPIEGELUNGSSATZ"

reste pour obtenir le résultat annoncé à "faire tendre n vers l'infini".

Bibliographie.

- [1] Fresnel J. Nombres de Bernouilli et fonctions L p-adiques,
Ann. Inst. Fourier, Grenoble, 17, 2 (1967).
- [2] Gras G. Annulation du groupe des ℓ -classes généralisées d'une
extension abélienne réelle de degré premier à ℓ .
A paraître aux Ann. Inst. Fourier (1979).
- [3] Leopoldt H. W. Zur Struktur der ℓ -Klassengruppe galoischer Zahl-
körper, Journal für die reine und Angew. Math. 199 (1958).
- [4] Oriat B. et Satgé Ph. Un essai de généralisation du "Spiegelungssatz",
à paraître.

Bernard Oriat
Mathématiques (ERA 07 06 54)
Faculté des Sciences
25030 BESANCON Cedex

SPIEGELUNGSSATZ ET $\mathbb{Z}_\ell$ -EXTENSIONS

Bernard ORLAT

Nous généralisons ici les définitions données par Iwasawa sous le nom de Δ -décomposition [2]. Si L/k est l'extension considérée, de groupe de Galois G , les paramètres λ_φ , μ_φ , ν_φ étaient associés à des idempotents de l'algèbre $\mathbb{Z}_\ell[G]$. Nous montrons ici que l'on peut les associer à des idéaux de l'algèbre $\mathbb{Z}_\ell[G]$. Ceci permet de ne pas utiliser l'hypothèse " ℓ est premier au degré de L/k ". Nous généralisons ainsi les inégalités : $\lambda_\varphi \leq \lambda^-$ et $\lambda^+ \leq \lambda^-$, énoncées dans [2].

DEFINITIONS ET NOTATIONS

Soient L/k une extension abélienne finie de corps de nombres, G son groupe de Galois, ℓ un nombre premier impair.

Soit k_∞/k une $\mathbb{Z}_\ell$ -extension de k . On note k_r le sous-corps de k_∞ tel que $[k_r : k] = \ell^r$ et i l'unique entier tel que $k_i = k_\infty \cap L$. On pose $L_r = k_{r+i} L$ et $L_\infty = \bigcup_{r \geq 0} L_r$. Ainsi L_∞/L est une $\mathbb{Z}_\ell$ -extension et $[L_r : L] = \ell^r$.

Soit H le sous-groupe de G , défini par $H = \text{Gal}(L/k_i)$.

On désigne par I un idéal de $\mathbb{Z}_\ell[G]$ et on pose $I_0 = I \cap \mathbb{Z}_\ell[H]$. Soit $\text{Ker } I_0$ l'ensemble des σ de H tels que $\sigma - 1$ appartienne à I_0 . C'est un sous-groupe de H et K_I est le corps intermédiaire entre k_i et L défini par l'égalité : $\text{Ker } I_0 = \text{Gal}(L/K_I)$.

Pour tout entier r , on pose $K_{I,r} = k_{r+i} K_I$ et $K_{I,\infty} = \bigcup_{r \geq 0} K_{I,r}$. Il est clair que $K_{I,\infty}/K_I$ est une $\mathbb{Z}_\ell$ -extension et que $[K_{I,r} : K_I] = \ell^r$.

Soit $H_r = \text{Gal}(L_r/k_{i+r})$. Ce groupe est isomorphe à H . Nous notons I_r l'image de I_0 dans l'isomorphisme $\mathbb{Z}_\ell[H] \cong \mathbb{Z}_\ell[H_r]$.

Soit $\mathcal{K}(K_{I,r})$ le ℓ -groupe des classes d'idéaux de $K_{I,r}$. C'est un $\mathbb{Z}_\ell[H_r]$ -module, ou compte tenu de l'isomorphisme écrit ci-dessus, un $\mathbb{Z}_\ell[H]$ -module.

Soit $\mathcal{H}(K_{I,r})^{I_0}$ le sous-groupe de $\mathcal{H}(K_{I,r})$ engendré par les éléments de la forme h^x ; h parcourant $\mathcal{H}(K_{I,r})$ et x parcourant I_0 . On désigne par $\mathcal{H}_r^I$ le quotient $\mathcal{H}(K_{I,r}) / \mathcal{H}(K_{I,r})^{I_0}$. C'est donc le plus grand quotient de $\mathcal{H}(K_{I,r})$ annulé par I_0 .

THEOREME DE STRUCTURE

Notons Γ_r le groupe de Galois de $K_{I,r}/K_I$. C'est un groupe cyclique d'ordre ℓ^r . Désignons par Γ la limite projective des groupes Γ_r , relativement aux homomorphismes de restriction. C'est le groupe de Galois de $K_{I,\infty}/K_I$; il est isomorphe au groupe additif $\mathbb{Z}_\ell$. On note γ un $\mathbb{Z}_\ell$ -générateur ce groupe. Soit $\mathcal{C}(I)$ la limite projective des groupes de classes d'idéaux $\mathcal{H}(K_{I,r})$ relativement aux normes. Comme $\mathcal{H}(K_{I,r})$ est un $\mathbb{Z}_\ell[\Gamma_r]$ -module, $\mathcal{C}(I)$ est un module sur $\varprojlim \mathbb{Z}_\ell[\Gamma_r]$. Rappelons que cet anneau est isomorphe à $\Lambda = \mathbb{Z}_\ell[[T]]$, anneau des séries formelles à coefficients dans $\mathbb{Z}_\ell$. Donc $\mathcal{C}(I)$ est un Λ -module. La théorie classique [3] montre que $\mathcal{C}(I)$ est un Λ -module de type fini et qu'il existe des éléments $\tau_1, \dots, \tau_s$ dans $\mathcal{C}(I)$ tels que $\mathcal{H}(K_{I,r})$ soit isomorphe, dès que

$$K_{I,r+1}/K_{I,r} \text{ est ramifiée, à } \mathcal{C}(I) / [\mathcal{C}(I)^{\gamma-1} \tau_1^{\mathbb{Z}_\ell} \dots \tau_s^{\mathbb{Z}_\ell}]^{1+\gamma+\dots+\gamma^{\ell^r-1}}.$$

Mais $\mathcal{C}(I)$ est aussi un $\mathbb{Z}_\ell[H]$ -module. Soit $\mathcal{C}(I)^{I_0}$ le sous-module de $\mathcal{C}(I)$ engendré par les éléments de la forme c^x , c parcourant $\mathcal{C}(I)$ et x parcourant I_0 . Posons $\mathcal{C}^I = \mathcal{C}(I) / \mathcal{C}(I)^{I_0}$. Ainsi, $\mathcal{C}^I$ est le plus grand quotient de $\mathcal{C}(I)$, annulé par I_0 . Soient $\bar{\tau}_1, \dots, \bar{\tau}_s$ les classes des éléments $\tau_1, \dots, \tau_s$ modulo $\mathcal{C}(I)^{I_0}$.

Théorème : le module quotient $\mathcal{C}^I$ défini ci-dessus est un Λ -module de type fini. Dès que l'extension $K_{I,r+1}/K_{I,r}$ est ramifiée, nous avons un isomorphisme :

$$\mathcal{H}_r^I \cong \mathcal{C}^I / ((\mathcal{C}^I)^{\gamma-1} \bar{\tau}_1^{\mathbb{Z}_\ell} \dots \bar{\tau}_s^{\mathbb{Z}_\ell})^{1+\gamma+\dots+\gamma^{\ell^r-1}}.$$

Démonstration : La première affirmation est évidente. Supposons, pour simplifier les notations, que $K_{I,1}/K_I$ soit ramifiée. Pour tout entier r , soit M_r la ℓ -

extension non ramifiée, abélienne, maximale de $K_{I,r}$. Soit $M_\infty = \bigcup_{r \geq 0} M_r$. On sait que $\mathcal{G}(I)$ est le groupe de Galois de $M_\infty/K_{I,\infty}$ et que $\mathcal{G}(I)^{\gamma-1} \tau_1^{\mathbb{Z}_\ell} \dots \tau_s^{\mathbb{Z}_\ell}$ est le groupe de Galois de $M_\infty/K_{I,\infty} M_0$ [3]. Ces considérations expliquent l'isomorphisme $\mathcal{H}(K_I) = \mathcal{G}(I) / \mathcal{G}(I)^{\gamma-1} \tau_1^{\mathbb{Z}_\ell} \dots \tau_s^{\mathbb{Z}_\ell}$. Mais de plus $\mathcal{H}(K_I)$ est un $\mathbb{Z}_\ell[H]$ -module. Il en est donc de même $\text{Gal}(K_{I,\infty} M_0 / K_{I,\infty})$. Donc $\mathcal{G}(I)^{\gamma-1} \tau_1^{\mathbb{Z}_\ell} \dots \tau_s^{\mathbb{Z}_\ell}$ est un sous- $\mathbb{Z}_\ell[H]$ -module de $\mathcal{G}(I)$ et l'isomorphisme écrit ci-dessus est un isomorphisme de $\mathbb{Z}_\ell[H]$ -modules. Dans cet isomorphisme, $\mathcal{H}(K_I)^{I_0}$ correspond à $(\mathcal{G}(I)^{I_0} \mathcal{G}(I)^{\gamma-1} \tau_1^{\mathbb{Z}_\ell} \dots \tau_s^{\mathbb{Z}_\ell}) / (\mathcal{G}(I)^{\gamma-1} \tau_1^{\mathbb{Z}_\ell} \dots \tau_s^{\mathbb{Z}_\ell})$. On en déduit, en passant au quotient, l'isomorphisme annoncé. Si maintenant, on suppose que $K_{I,r+1}/K_{I,r}$ est ramifiée, alors on peut répéter le même raisonnement, en remplaçant γ par γ^{ℓ^r} . L'élément τ_u de $\mathcal{G}(I)$ est alors remplacé par $\tau_u^{1+\gamma+\dots+\gamma^{\ell^r-1}}$.

Les résultats classiques concernant les Λ -modules de type fini permettent de déduire de ce théorème la définition de μ_I , λ_I et ν_I .

Définition : Il existe des entiers positifs μ_I , λ_I et un entier ν_I , tels que, pour r assez grand, l'ordre de $\mathcal{H}_r^I$ soit de la forme

$$|\mathcal{H}_r^I| = \ell^{\mu_I \ell^r + \lambda_I r + \nu_I}.$$

SPIEGELUNGSSATZ

On conserve les mêmes données. On suppose de plus que L contient une racine primitive $\ell^{\text{ème}}$ de 1, notée ζ_ℓ . Soit χ^{**} l'homomorphisme de $G = \text{Gal}(L/k)$ dans $\mathbb{Z}_\ell^*$, groupe des unités de $\mathbb{Z}_\ell$, défini par $\zeta_\ell^\sigma = \zeta_\ell^{\chi^{**}(\sigma)}$, pour tout σ de G . On associe à χ^{**} l'involution de l'algèbre $\mathbb{Z}_\ell[G]$, qui à tout élément $x = \sum_{\sigma \in G} a_\sigma \sigma$ de $\mathbb{Z}_\ell[G]$, associe l'élément $\bar{x} = \sum_{\sigma \in G} a_\sigma \chi^{**}(\sigma) \sigma^{-1}$. On note $\bar{I}$ (resp. $\bar{I}_0$) l'image de I (resp. I_0) par cette involution. Il est évident que $\bar{I}_0 = \bar{I} \cap \mathbb{Z}_\ell[H]$. A l'idéal

$\bar{I}$ on associe, comme pour I , les corps $K_{\bar{I}}$, $K_{\bar{I},r}$, $K_{\bar{I},\infty}$ et les groupes de classes d'idéaux $\mathcal{K}_{\bar{I},r}$.

Lemme : On a les égalités : $K_I(\zeta_\ell) = K_{\bar{I}}(\zeta_\ell) = K_I K_{\bar{I}}$ et $k_i = k_\infty \cap K_I = k_\infty \cap K_{\bar{I}}$.

Démonstration : Le groupe de Galois de $L/k(\zeta_\ell)$ est le noyau de χ^{**} . L'égalité : $K_I(\zeta_\ell) = K_{\bar{I}}(\zeta_\ell)$ est équivalente à l'égalité : $\text{Ker } I_0 \cap \text{Ker } \chi^{**} = \text{Ker } \bar{I}_0 \cap \text{Ker } \chi^{**}$ qui est facile à vérifier. De même on vérifie aussi que $\text{Ker } I_0 \cap \text{Ker } \bar{I}_0$ est égal à $\text{Ker } I_0 \cap \text{Ker } \chi^{**}$. Ceci montre que $K_I K_{\bar{I}} = K_I(\zeta_\ell)$. On déduit de ces égalités que $[K_I : K_I \cap K_{\bar{I}}]$ et $[K_{\bar{I}} : K_I \cap K_{\bar{I}}]$ sont premiers à ℓ . D'où les égalités : $k_i = k_\infty \cap K_I = k_\infty \cap K_I \cap K_{\bar{I}} = k_\infty \cap K_{\bar{I}}$.

On suppose désormais que k_∞/k est la $\mathbb{Z}_\ell$ -extension cyclotomique de k . Pour tout r , nous prolongeons χ^{**} à $\text{Gal}(L_r/k)$, en utilisant la même définition ; c'est-à-dire $\zeta_\ell^\sigma = \zeta_\ell^{\chi^{**}(\sigma)}$.

Lemme : Si r est un entier positif, soit $n = \ell^{r+i+1}$. Alors L_r contient une racine primitive $n^{\text{ème}}$ de 1, notée ζ_n . Pour tout σ de $H_r = \text{Gal}(L_r/k_{r+i})$ nous avons l'égalité :

$$\zeta_n^\sigma = \zeta_n^{\chi^{**}(\sigma)}.$$

Démonstration : La première assertion découle du fait que k_∞/k est la $\mathbb{Z}_\ell$ -extension cyclotomique de k . Notons A_n l'anneau $\mathbb{Z}/n\mathbb{Z}$ et A_n^* le groupe des classes d'entiers modulo n , premières à n . Soit χ^* l'homomorphisme de H_r dans A_n^* défini par l'égalité $\zeta_n^\sigma = \zeta_n^{\chi^*(\sigma)}$. Le noyau de χ^* est $\text{Gal}(L_r/k_{r+i}(\zeta_n))$. Mais le degré de $k_{i+r}(\zeta_n)/k_{i+r}$ est un diviseur de $\ell-1$. Donc $\chi^{*\ell-1} = 1$. D'autre part, nous avons $\chi^*(\sigma) \equiv \chi^{**}(\sigma) \pmod{\ell}$ et $\chi^{**}(\sigma)$ est évidemment une racine $(\ell-1)^{\text{ème}}$ de 1. Donc $\chi^*(\sigma)$, pour tout σ de H_r , est le résidu modulo n de $\chi^{**}(\sigma)$.

Il découle de ce lemme, que si nous essayons d'appliquer le théorème 1 de [4] dans l'extension L_r/k_{r+i} de groupe de Galois H_r , avec $n = \ell^{r+i+1}$, alors les résidus modulo n des idéaux I_r et $\bar{I}_r$ se correspondent dans l'involution de $A_n^*[H_r]$ définie à partir de χ^* .

Proposition : Soit r un entier positif et n la puissance de ℓ , définie par $n = \ell^{r+1}$. Soit I_r' l'idéal de $A_n[H_r]$ résidu modulo n de I_r . Pour r assez grand, le corps $K_{I_r'}$ défini, ainsi qu'en [4], comme corps intermédiaire entre L_r et K_{r+1} à l'aide de l'idéal I_r' coïncide avec le corps K_{I_r} défini plus haut. Le groupe $\mathcal{H}_{I_r}'$ de classes d'idéaux, défini ainsi qu'en [4] comme associé à l'idéal I_r' de $A_n[H_r]$ est égal à $\mathcal{H}_{I_r}^I / (\mathcal{H}_{I_r}^I)^n$. Ainsi, pour toute puissance de ℓ notée m , comprise entre ℓ et n , on a $\dim_m \mathcal{H}_{I_r}' = \dim_m \mathcal{H}_{I_r}^I$.

Démonstration : Soit $\text{Ker } I_r = \{\sigma ; \sigma \in H_r ; \sigma - 1 \in I_r\}$. Il s'agit donc d'un sous-groupe de H_r et $\text{Gal}(L_r/K_{I_r})$ est égal à $\text{Ker } I_r$. L'ordre de ce sous-groupe ne dépend pas de r , car $\text{Ker } I_r$ correspond à $\text{Ker } I_0$ dans l'isomorphisme $H_r \cong H$. Soit $\text{Ker } I_r' = \{\sigma ; \sigma \in H_r ; \sigma - 1 \in I_r'\}$. Par définition, on a $\text{Ker } I_r' = \text{Gal}(L_r/K_{I_r'})$. Il est clair que $\text{Ker } I_r' \supset \text{Ker } I_r$ et que par l'isomorphisme $H_r \cong H_{r+1}$, l'image de $\text{Ker } I_{r+1}'$ est incluse dans $\text{Ker } I_r'$. Ainsi pour r assez grand, $\text{Ker } I_r'$ est d'ordre constant.

Soit σ un élément de H et pour tout r , désignons par σ_r son image par l'isomorphisme $H \cong H_r$. Supposons que pour tout r , σ_r appartienne à $\text{Ker } I_r'$. Cela veut dire, que pour tout r , il existe a_r dans I_r tel que $\sigma_r - 1 \equiv a_r \pmod{n}$. Soit b_r l'élément de I_0 correspondant à a_r par l'isomorphisme $\mathbb{Z}_\ell[H_r] \cong \mathbb{Z}_\ell[H]$. Nous avons donc $\sigma - 1 \equiv b_r \pmod{n}$. La suite $(b_r)_{r \geq 0}$ est donc une suite d'éléments de I_0 , convergente vers $\sigma - 1$. Comme I_0 est un fermé de $\mathbb{Z}_\ell[H]$, on en déduit que $\sigma - 1$ appartient à I_0 . Donc σ appartient à $\text{Ker } I_0$ et σ_r appartient à $\text{Ker } I_r$. Ceci démontre donc, qu'à partir d'un certain rang, on a $\text{Ker } I_r = \text{Ker } I_r'$. Le reste de la démonstration est évident.

Théorème : On suppose que k_∞/k est la $\mathbb{Z}_\ell$ -extension cyclotomique de k et que $L/\mathbb{Q}$ est abélienne. On suppose aussi que L contient une racine primitive $\ell^{\text{ème}}$ de 1. Supposons enfin que K_I est réel. Alors, on a l'inégalité : $\lambda_I \leq \lambda_{\bar{I}}$.

Démonstration : Soit r un entier assez grand pour que la proposition précédente soit vérifiée à la fois pour I et pour $\bar{I}$. Appliquons le théorème 1 de [4] à l'exten-

sion L_r/k_{r+i} , avec $n = \ell^{r+i+1}$. Soient $E(K_{\bar{I}, r})$ le groupe des unités de $K_{\bar{I}, r}$, $\mathcal{E}(K_{\bar{I}, r})$ le quotient $E(K_{\bar{I}, r})/E(K_{\bar{I}, r})^n$, $\mathcal{E}_{\bar{I}}$ le sous-module de $\mathcal{E}(K_{\bar{I}, r})$ annulé par $\bar{I}_0$ et enfin $\mathcal{E}_{\bar{I}}^0$ le sous-module de $\mathcal{E}_{\bar{I}}$ engendré par les classes d'unités n -primaires sur $K_{\bar{I}, r}$. Si $\mathcal{X}_{\bar{I}, r}$ est le sous-module de $\mathcal{X}(K_{\bar{I}, r})$ formé des éléments h de $\mathcal{X}(K_{\bar{I}, r})$ annulé par $\bar{I}_0$, alors on déduit de la proposition précédente et de [4], les inégalités : $\dim_m \mathcal{X}_{\bar{I}, r}^{\bar{I}} - \dim_m \mathcal{X}_{\bar{I}, r} \leq \dim_{\ell} \mathcal{E}_{\bar{I}}^0$, pour toute puissance de ℓ , notée m et comprise entre ℓ et n .

Montrons d'abord que $\mathcal{E}_{\bar{I}}^0$ est réduit à 1. Pour cela, on introduit la conjugaison complexe de $L/\mathbb{Q}$ notée σ_{∞} . C'est un élément de H . Notons de la même façon l'élément de H_r qui lui correspond. Comme K_I est réel, $\sigma_{\infty}-1$ appartient à I_0 et $\sigma_{\infty}+1$ appartient donc à $\bar{I}_0$. En décomposant $\mathcal{E}(K_{\bar{I}, r})$ à l'aide des idempotents $(1+\sigma_{\infty})/2$ et $(1-\sigma_{\infty})/2$, on constate que $\mathcal{E}_{\bar{I}}$ est, ou bien réduit à 1, ou bien cyclique et engendré par la classe d'une racine de l'unité. Mais pour r assez grand, $K_{\bar{I}, r+1}/K_{\bar{I}, r}$ est ramifiée. Dans ce cas, on a donc $\mathcal{E}_{\bar{I}}^0 = 1$. Ainsi, nous avons montré que pour r assez grand, l'inégalité : $\dim_m \mathcal{X}_{\bar{I}, r}^{\bar{I}} \leq \dim_m \mathcal{X}_{\bar{I}, r}$ est vérifiée.

Il reste maintenant à comparer $\mathcal{X}_{\bar{I}, r}$ et $\mathcal{X}_{\bar{I}, r}^{\bar{I}}$. Pour cela, considérons l'application α_r de $\mathcal{X}_{\bar{I}, r}$ dans $\mathcal{X}_{\bar{I}, r}^{\bar{I}}$, restriction de l'application canonique de $\mathcal{X}(K_{\bar{I}, r})$ sur $\mathcal{X}_{\bar{I}, r}^{\bar{I}}$. Son noyau est $\mathcal{X}_{\bar{I}, r} \cap \mathcal{X}(K_{\bar{I}, r})^{\bar{I}_0}$. Nous allons montrer que l'ordre de ce noyau est borné. Pour cela introduisons l'idéal V de $\mathbb{Z}_{\ell}[H]$ défini par $V = \{x ; x \in \mathbb{Z}_{\ell}[H] ; x\bar{I}_0 = 0\}$ et les idéaux $\mathbb{Q}_{\ell}\bar{I}_0$ et $\mathbb{Q}_{\ell}V$ de $\mathbb{Q}_{\ell}[H]$. Il est facile de vérifier que $\mathbb{Q}_{\ell}[H]$ est somme directe de ces deux idéaux. On en déduit alors l'existence d'un entier a indépendant de r tel que ℓ^a appartienne $\bar{I}_0 + V$. Ainsi cet élément ℓ^a annule le noyau de α_r . D'autre part, utilisons le résultat " $\mu = 0$ " [1]. Il montre en particulier que $\mu_I = \mu_{\bar{I}} = 0$. Mais il montre aussi que le ℓ -rang du groupe $\mathcal{X}(K_{\bar{I}, r})$ est borné. Il en sera de même du ℓ -rang du noyau de α_r .

Ainsi, nous avons vérifié que l'ordre de ce noyau est borné.

Nous pouvons déduire des considérations qui précèdent qu'il existe une constante c telle que pour n assez grand et pour toutes puissances de ℓ , m_1 et m_2 vérifiant $m_1 \leq m_2 \leq n$, on ait l'inégalité :

$$\sum_{m_1 \leq m \leq m_2} \dim_m \mathcal{H}_r^I \leq c + \sum_{m_1 \leq m \leq m_2} \dim_m \mathcal{H}_r^{\bar{I}}$$

(les deux sommes sont étendues aux puissances de ℓ comprises entre m_1 et m_2).

D'autre part on déduit de la théorie classique des Λ -modules de type fini et du théorème précédent, que si m est une puissance de ℓ assez grande, alors

λ_I est égal à $\lim_{r \rightarrow \infty} \dim_m \mathcal{H}_r^I$. Sous la même condition on a aussi

$\lambda_{\bar{I}} = \lim_{r \rightarrow \infty} \dim_m \mathcal{H}_r^{\bar{I}}$. Il est aisé de vérifier que les inégalités écrites ci-dessus

ne sont possibles que si $\lambda_I \leq \lambda_{\bar{I}}$.

B I B L I O G R A P H I E

=====

- [1] B. FERRERO and L. C. WASHINGTON - The Iwasawa invariant μ_p vanishes for abelian number fields, Annals of Math., vol. 109 (1979).
- [2] K. IWASAWA - On the theory of cyclotomic fields, Annals of Math., vol. 70 n° 3 (1959).
- [3] S. LANG - Cyclotomic fields, Springer-Verlag (1978).
- [4] B. ORLAT et Ph. SATGE - Un essai de généralisation du Spiegelungssatz, J. für die reine und ang. Math. 307/308 (1979).

Bernard ORLAT
Mathématiques
(E. R. A. n° 070654)
Faculté des Sciences
25030 BESANCON CEDEX

ANNULATION DE GROUPE DE CLASSES REELLES. =====

Bernard Oriat.

Introduction.

Il est bien connu que le groupe des classes relatives d'une extension abélienne du corps des rationnels est annulé par tout élément entier de l'idéal de Stickelberger. Soit ℓ un nombre premier impair. Nous montrons dans les pages qui suivent qu'un certain groupe de ℓ -classes réelles $\mathcal{K}(\chi)$, associé à un caractère χ d'ordre g et considéré comme $\mathbb{Z}_{\ell}^{(g)}$ -module est annulé par la valeur en 1 de la fonction L ℓ -adique : $L_{\ell}(1, \chi)$, ou bien par un multiple bien défini de cette valeur. Pour l'essentiel, la méthode employée consiste à transposer par "Spiegelungssatz" le théorème d'annulation de Stickelberger. Cette méthode a été introduite par Georges Gras dans [3]. La démonstration donnée ici semble un peu plus simple et le résultat obtenu plus général : on ne fait plus ici l'hypothèse " ℓ premier à g ".

1. Notations et définitions.

On désigne par ℓ un nombre premier impair. Soit χ un caractère résiduel d'ordre g et de conducteur f , réel, différent du caractère unité. On note $K/\mathbb{Q}$ l'extension cyclique, de corps de base le corps des rationnels $\mathbb{Q}$, correspondant à χ . Nous voulons dire par là, que si l'on considère χ comme un homomorphisme de $\text{Gal}(\mathbb{Q}^{(f)}/\mathbb{Q}) = (\mathbb{Z}/f\mathbb{Z})^*$ dans le groupe des racines $g^{\text{ème}}$ de l'unité, alors le noyau de χ est le groupe de Galois $\text{Gal}(\mathbb{Q}^{(f)}/K)$. On désigne par G le groupe de Galois de $K/\mathbb{Q}$. Le caractère χ peut aussi être considéré comme un homomorphisme de G dans $\mathbb{Q}_{\ell}^{(g)*}$, groupe multiplicatif du corps $\mathbb{Q}_{\ell}^{(g)}$; ce corps est le corps obtenu en ajoutant au corps ℓ -adique $\mathbb{Q}_{\ell}$, les racines $g^{\text{ème}}$ de l'unité. On désigne par χ_1 le

prolongement $\mathbb{Z}_\ell$ -linéaire de χ à $\mathbb{Z}_\ell[G]$. Le noyau de χ_1 est un idéal de $\mathbb{Z}_\ell[G]$ qui peut être défini à l'aide d'un idempotent de l'algèbre $\mathbb{Q}_\ell[G]$ de la façon suivante : Soit ψ le caractère ℓ -adique issu de χ , c'est-à-dire la trace de χ dans l'extension $\mathbb{Q}_\ell^{(g)}/\mathbb{Q}_\ell$. Soit $1_\psi = (1/|G|) \sum_{\tau \in G} \psi(\tau^{-1}) \tau$ l'idempotent de $\mathbb{Q}_\ell[G]$ associé à ψ . Alors $\text{Ker } \chi_1$ est l'ensemble des x de $\mathbb{Z}_\ell[G]$ tels que $x 1_\psi = 0$. Une autre façon de définir $\text{Ker } \chi_1$ est utilisée dans la suite : désignons par σ un générateur de G et par $P(Y)$ le polynôme $\prod (Y - \chi(\sigma)^u)$, u parcourant le groupe $\text{Gal}(\mathbb{Q}_\ell^{(g)}/\mathbb{Q}_\ell)$. Il s'agit du polynôme cyclotomique ℓ -adique ayant $\chi(\sigma)$ comme racine. L'idéal $\text{Ker } \chi_1$ est l'idéal de $\mathbb{Z}_\ell[G]$ engendré par $P(\sigma)$. Remarquons aussi que χ_1 a pour image $\mathbb{Z}_\ell^{(g)}$, anneau des entiers de $\mathbb{Q}_\ell^{(g)}$. On a donc un isomorphisme d'anneaux entre $\mathbb{Z}_\ell[G]/\text{Ker } \chi_1$ et $\mathbb{Z}_\ell^{(g)}$. Cet isomorphisme fait correspondre à la classe de $\sum_{\tau \in G} a_\tau \tau$ modulo $\text{Ker } \chi_1$, l'élément $\sum_{\tau \in G} a_\tau \chi(\tau)$ de $\mathbb{Z}_\ell^{(g)}$. Ainsi tout $\mathbb{Z}_\ell[G]$ -module annihilé par $\text{Ker } \chi_1$ peut être considéré comme un $\mathbb{Z}_\ell^{(g)}$ -module.

D'une façon générale, dans toute la suite, si A/B est une extension galoisienne et si C est un corps intermédiaire tel que A/C soit abélienne, et C/B galoisienne, on entend par opération de $\text{Gal}(C/B)$ sur $\text{Gal}(A/C)$, l'opération conjugaison ainsi notée : Si u appartient à $\text{Gal}(A/C)$ et si τ appartient à $\text{Gal}(C/B)$, alors u^τ est égal à $t^{-1} u t$, où t est un prolongement de τ à A . Précisons de plus que si a appartient à A , on désigne par a^u l'image de a par u et, en conséquence, la composition des automorphismes u et v de A est notée suivant la convention $a^{(uv)} = (a^u)^v$.

Soit U/K la ℓ -extension abélienne maximale de K , non ramifiée en dehors de ℓ . Le groupe de Galois $\text{Gal}(U/K)$ est un $\mathbb{Z}_\ell[G]$ -module. Soit K_∞ la $\mathbb{Z}_\ell$ -extension maximale de K (Comme K est réel, il s'agit donc de la $\mathbb{Z}_\ell$ -extension cyclotomique de K). On sait que $\text{Gal}(U/K_\infty)$ est le sous-module de torsion de $\text{Gal}(U/K)$ et qu'il est fini. Nous désignons par $\mathcal{H}(\chi)$ le $\mathbb{Z}_\ell[G]$ -module quotient $\text{Gal}(U/K_\infty)/\text{Gal}(U/K_\infty)^{P(\sigma)}$. Il s'agit donc d'un $\mathbb{Z}_\ell^{(g)}$ -module.

2. Enoncé des résultats obtenus.

Rappelons que χ est un caractère réel, différent du caractère unité et que g est son ordre.

Théorème A. Si g n'est pas une puissance de ℓ , alors $\mathcal{H}(\chi)$ est annihilé en tant que $\mathbb{Z}_{\ell}^{(g)}$ -module par $L_{\ell}(1, \chi)$, valeur en 1 de la fonction L ℓ -adique relative à χ .

Théorème B. Si g est une puissance de ℓ et si ζ_g est une racine primitive $g^{\text{ème}}$ de 1, alors $\mathcal{H}(\chi)$ est annihilé par $(1 - \zeta_g)L_{\ell}(1, \chi)$.

3. Démonstration des théorèmes.

Soit N le corps intermédiaire entre U et K tel que $\text{Gal}(U/N) = \text{Gal}(U/K)^{P(\sigma)}$. Ainsi N/K est la ℓ -extension abélienne, non ramifiée sauf en ℓ , maximale telle que $N/\mathbb{Q}$ soit galoisienne et $\text{Gal}(N/K)$ soit annihilé par $P(\sigma)$. Soit, pour tout entier n , $\mathbb{Q}_n$ le sous-corps de $\mathbb{Q}(\ell^n)$ défini par $[\mathbb{Q}(\ell^n) : \mathbb{Q}_n] = \ell - 1$. Pour tout corps A , on pose $A_i = A \cap \mathbb{Q}_i$. On désigne par $\mathbb{Q}_{\infty} = \bigcup_{i \geq 1} \mathbb{Q}_i$ et $K_{\infty} = \bigcup_{i \geq 1} K_i = K \cap \mathbb{Q}_{\infty}$ les $\mathbb{Z}_{\ell}$ -extensions cyclotomiques de $\mathbb{Q}$ et K . Soit n_0 l'entier non nul défini par $\mathbb{Q}_{n_0} = \mathbb{Q}_{\infty} \cap K$. On a donc $K_{n_0} = K \neq K_{n_0+1}$.

Proposition 3.1. Si g n'est pas une puissance de ℓ , l'intersection $N \cap K_{\infty}$ est égale à K . Si g est une puissance de ℓ alors $N \cap K_{\infty}$ est égal à K_{n_0+1} . Dans tous les cas, $\mathcal{H}(\chi)$ est isomorphe, en tant que $\mathbb{Z}_{\ell}^{(g)}$ -module, à $\text{Gal}(N/N \cap K_{\infty})$.

Démonstration. Comme l'extension $N \cap K_\infty / \mathbb{Q}$ est abélienne, le $\mathbb{Z}_\ell[G]$ -module $\text{Gal}(N \cap K_\infty / K)$ est annulé par $\sigma - 1$ et $P(\sigma)$. Donc il est annulé par $P(1)$. Si g n'est pas une puissance de ℓ , alors $P(1)$ est une unité de $\mathbb{Z}_\ell$ et $N \cap K_\infty = K$. Si par contre, g est une puissance de ℓ , alors $P(1) = \ell$ et le degré $[N \cap K_\infty : K]$ ne peut excéder ℓ . Nous avons donc $N \cap K_\infty \subset K_{n_0+1}$. D'autre part, l'extension $K_{n_0+1} / \mathbb{Q}$ est abélienne et $\text{Gal}(K_{n_0+1} / K)$ est annulé par $\sigma - 1$ et $\ell = P(1)$, donc par $P(\sigma)$. Ainsi, on a $K_{n_0+1} = N \cap K_\infty$.

Démontrons maintenant l'égalité $\text{Gal}(U/K)^{P(\sigma)} \cap \text{Gal}(U/K_\infty) = \text{Gal}(U/K_\infty)^{P(\sigma)}$. Soit h un élément de $\text{Gal}(U/K)$ et supposons que $h^{P(\sigma)}$ appartienne à $\text{Gal}(U/K_\infty)$. Comme $\text{Gal}(U/K_\infty)$ est le sous-module de torsion de $\text{Gal}(U/K)$, il existe un entier k tel que $h^{\ell^k P(\sigma)} = 1$. Mais $K_\infty / \mathbb{Q}$ est abélienne et $h^{\ell^k P(1)}$ appartient à $\text{Gal}(U/K_\infty)$. Donc h appartient lui-même à $\text{Gal}(U/K_\infty)$. Nous en déduisons les égalités et isomorphismes :

$$\begin{aligned} \mathcal{H}(X) &= \text{Gal}(U/K_\infty) / \text{Gal}(U/K_\infty)^{P(\sigma)} = \text{Gal}(U/K_\infty) / (\text{Gal}(U/K)^{P(\sigma)} \cap \text{Gal}(U/K_\infty)) \\ &\simeq (\text{Gal}(U/K)^{P(\sigma)} \text{Gal}(U/K_\infty)) / \text{Gal}(U/K)^{P(\sigma)} = \text{Gal}(U/N \cap K_\infty) / \text{Gal}(U/N) \\ &\simeq \text{Gal}(N/N \cap K_\infty). \end{aligned}$$

Ce qui termine la démonstration de la proposition 3.1.

Soit n un entier non nul. Définissons N^n comme le corps intermédiaire entre N et $N \cap K_\infty$ maximal tel que $\text{Gal}(N^n / N \cap K_\infty)$ soit d'exposant divisant ℓ^n . Alors $\mathcal{H}(X) / \mathcal{H}(X)^{\ell^n}$ est isomorphe en tant que $\mathbb{Z}_\ell[G]$ -module à $\text{Gal}(N^n / N \cap K_\infty)$. Introduisons L , corps obtenu en ajoutant à K les racines $\ell^{\text{ème}}$ de 1 ; c'est-à-dire $L = K\mathbb{Q}^{(\ell)}$, et $M^n = N^n L = N^n \mathbb{Q}^{(\ell)}$. Nous avons alors

$M_n^n = M_n^n \mathbb{Q}_n = N_n^n L_n = N_n^n \mathbb{Q}(\ell^n)$. Soit G_n le groupe de Galois $\text{Gal}(L_n/\mathbb{Q})$. Il est clair que tous les G -modules introduits précédemment peuvent également être considérés comme des G_n -modules.

Proposition 3. 2. On suppose que n est un entier non nul. Si g est une puissance de ℓ , on suppose de plus n supérieur à $n_0 + 1$. Alors

$\mathcal{H}(X)/\mathcal{H}(X)^{\ell^n}$ est isomorphe en tant que G_n -module à $\text{Gal}(M_n^n/L_n)$.

Démonstration. Nous avons $M_n^n = N_n^n L_n$. D'autre part, on vérifie l'égalité $N_n^n \cap L_n = N \cap K_\infty$. On en déduit l'isomorphisme $\text{Gal}(M_n^n/L_n) \simeq \text{Gal}(N_n^n/N \cap K_\infty)$; d'où le résultat en utilisant la proposition 3. 1.

L'extension M_n^n/L_n est une extension de Kummer d'exposant divisant ℓ^n . Nous notons W_n son radical, c'est-à-dire :
 $W_n = \{w; w \in L_n; \sqrt[n]{w} \in M_n^n\}$. Le groupe $W_n/(L_n^*)^{\ell^n}$ est évidemment un G_n -module et en tant que groupe il est isomorphe à $\text{Gal}(M_n^n/L_n)$. Les structures de G_n -modules de ces deux groupes sont liées par l'involution du miroir que nous allons rappeler :

Soit $A_n = \mathbb{Z}/\ell^n \mathbb{Z}$ l'anneau des classes résiduelles d'entiers modulo ℓ^n et A_n^* son groupe multiplicatif. Si ξ_n est une racine primitive $(\ell^n)^{\text{ème}}$ de 1, alors on note χ^* l'homomorphisme de G_n dans A_n^* défini par $\xi_n^\tau = \xi_n^{\chi^*(\tau)}$. Si $x = \sum_{\tau \in G} a_\tau \tau$ est un élément de $A_n[G_n]$, on pose $\bar{x} = \sum_{\tau \in G} a_\tau \chi^*(\tau) \tau^{-1}$. L'application de l'algèbre $A_n[G_n]$ dans elle-même qui à x fait correspondre $\bar{x}$ est

un automorphisme involutif de $A_n[G_n]$ que l'on appelle : "involution du miroir". Les groupes $\text{Gal}(M_n^n/L_n)$ et $W_n/(L_n^*)^{\ell^n}$ sont des $A_n[G_n]$ -modules et leurs structures sont liées par la proposition suivante :

Proposition 3.3. Les anneaux, dans $A_n[G_n]$, de $W_n/(L_n^*)^{\ell^n}$ et $\text{Gal}(M_n^n/L_n)$ sont images l'un de l'autre par l'involution du miroir.

Nous ne réécrivons pas ici la démonstration de la "Spiegelungs-relation" d'où provient ce résultat. On peut consulter [4] ou [5].

Introduisons n_1 et f_0 définis par l'égalité $f = \ell^{n_1} f_0$, f_0 étant premier à ℓ et f désignant le conducteur de χ (On a donc $n_1 \geq n_0$ sauf si $n_1 = 0$ et $n_0 = 1$). Posons $f_n = \ell^n f_0$ et supposons désormais n supérieur à n_1 . Alors f_n est le conducteur de L_n . On désigne par $\left(\frac{L_n}{a}\right)$ le symbole d'Artin attaché à l'extension $L_n/\mathbb{Q}$, a étant un entier premier à f_n . On considère l'élément de $\mathbb{Q}_\ell[G_n]$ défini par $s_n = (1/f_n) \sum_a \left(\frac{L_n}{a}\right)^{-1}$, la somme étant étendue aux entiers a de 1 à f_n et premiers à f_n . Rappelons le théorème de Stickelberger : l'idéal $s_n \mathbb{Z}_\ell[G_n] \cap \mathbb{Z}_\ell[G_n]$ de $\mathbb{Z}_\ell[G_n]$ annule le groupe des ℓ -classes d'idéaux (au sens ordinaire) de L_n . D'autre part nous utilisons également un élément s'_n défini par : $s'_n = s_n - \frac{1}{2} \sum_a \left(\frac{L_n}{a}\right)$, cette somme étant étendue aux entiers a de 1 à f_n et premiers à f_n . Si b est un entier premier à f_n , nous posons $y_n = \left(1 - b \left(\frac{L_n}{b}\right)^{-1}\right) s_n$ et $y'_n = \left(1 - b \left(\frac{L_n}{b}\right)^{-1}\right) s'_n$. La première quantité appartient à $\mathbb{Z}[G_n]$ et en imposant à b d'être impair, y'_n est aussi dans $\mathbb{Z}[G_n]$; ce que nous supposons dans la suite.

Proposition 3.4. On suppose toujours que n est un entier non nul, supérieur à n_1 . Si g est une puissance de ℓ , supposons de plus n supérieur à $n_0 + 1$. Alors $W_n/(L_n^*)^{\ell^n}$ est annulé par y'_n .

Démonstration. Soit w un élément de W_n . Comme l'extension

$L_n(\sqrt[n]{w})/L_n$ est non ramifiée, sauf en ℓ , l'idéal de L_n engendré par w est de la forme $\mathfrak{a}\ell^n b$, où $\mathfrak{a}$ est un idéal de L_n premier à ℓ et b un idéal de L_n dont la décomposition en idéaux premiers ne contient que des idéaux au-dessus de ℓ . Notons $\mathcal{I}(\ell)$ le groupe des idéaux engendré par les idéaux premiers de L_n au-dessus de ℓ , et D le groupe de décomposition de ℓ dans $L_n/\mathbb{Q}$. Le groupe $\mathcal{I}(\ell)$ est un $\mathbb{Z}[G_n]$ -module et plus précisément un $\mathbb{Z}[G_n/D]$ -module. Considérons l'élément s'_n de $\mathbb{Q}[G_n]$. Sa restriction à $\mathbb{Q}[G_n/D]$ est nulle d'après le théorème II 3 de [2]. Il en sera de même de la restriction de y'_n à $\mathbb{Z}[G_n/D]$ et y'_n annule le groupe $\mathcal{I}(\ell)$. Nous avons donc $b^{y'_n} = 1$.

D'autre part, on déduit du théorème de Stickelberger que $\mathfrak{a}^{y'_n}$ est principal. Il existe donc un élément u dans L_n et une unité ϵ de L_n tels que $w^{y'_n} = u\ell^n \epsilon$.

Introduisons maintenant la conjugaison complexe σ_∞ de G_n . Puisque K est réel, σ_∞ appartient à $\text{Gal}(L_n/K)$ et $\sigma_\infty - 1$ annule $\text{Gal}(M_n^n/L_n)$. Mais $\chi^*(\sigma_\infty) = -1$ et l'image de $\sigma_\infty - 1$ par l'involution du miroir est $-(\sigma_\infty + 1)$. On déduit de la proposition 3.2 que $\sigma_\infty + 1$ annule $W_n/(L_n^*)^{\ell^n}$. Cela implique que $\epsilon^{\sigma_\infty + 1}$ est une puissance $(\ell^n)^{\text{ème}}$ d'un élément de L_n , donc finalement d'une unité de L_n . Considérons le groupe des unités E de L_n et le quotient

$\mathcal{E} = E/E^{\ell^n}$. Ce groupe se décompose en produit direct sous la forme :
$$\mathcal{E} = \mathcal{E}^{(1+\sigma_\infty)/2} \mathcal{E}_n^{(1-\sigma_\infty)/2}$$
 Le premier facteur s'identifie par injection canonique à E_0/E_0 , où E_0 est le groupe des unités du sous-corps réel maximal de L_n . Le deuxième est cyclique, engendré par la classe d'une racine de l'unité. Ainsi, si $\epsilon^{\sigma_\infty + 1}$ appartient à E^{ℓ^n} , alors ϵ est, modulo E^{ℓ^n} , une racine de l'unité. Nous aurons donc $w^{y'_n} = v\ell^n \zeta$, avec v dans L_n et ζ racine de l'unité appartenant à L_n . Comme $n \geq n_1$, nous avons $L_n \neq L_{n+1}$ et $\zeta^{\ell^n} = 1$. Ceci montre que les racines $(\ell^n)^{\text{ème}}$ de $w^{y'_n}$ appartiennent à $M_n^n \cap L_{2n}$.

Il reste à calculer cette intersection : Nous avons

$M_n^n \cap L_{2n} = (L_n N^n) \cap L_{2n} = L_n(N^n \cap L_{2n})$. Si g n'est pas une puissance de

ℓ , on a $N^n \cap L_{2n} = K$. Si g est une puissance de ℓ , alors $N^n \cap L_{2n} = K_{n_0+1}$. D'où l'on déduit $M_n^n \cap L_{2n} = L_n K$ ou $L_n K_{n_0+1}$ suivant les cas. Mais si g est une puissance de ℓ , on a supposé $n \geq n_0 + 1$. Nous avons donc dans tous les cas $M_n^n \cap L_{2n} = L_n$. Ainsi $w_n^{y'}$ appartient à $(L_n^*)^{\ell^n}$; ce qui démontre la proposition 3.4.

Introduisons maintenant les éléments de $\mathbb{Q}_\ell[G_n]$:

$$x_n = \left(1 - b^{\varphi(\ell^n)} \left(\frac{L_n}{b}\right)\right) \left(1/f_n^{\varphi(\ell^n)}\right) \sum_a a^{\varphi(\ell^n)} \left(\frac{L_n}{a}\right),$$

$$x_n' = x_n - \frac{1}{2}(1-b) \sum_a a \left(\frac{L_n}{a}\right)^{-1}.$$

L'entier b est le même que précédemment. Il est seulement pour l'instant supposé premier à f_n et impair. L'indicateur d'Euler est noté φ et $\sum_a$ désigne la somme ^{sur} les entiers a , de 1 à f_n , premiers à f_n .

Proposition 3.5. Les éléments x_n et y_n appartiennent à $\mathbb{Z}_\ell[G_n]$. Leurs résidus modulo ℓ^n sont des éléments de $A_n[G_n]$, images l'un de l'autre par l'involution du miroir.

Démonstration. Le symbole $\sum_a$ désigne la somme ^{sur} les entiers a , de 1 à f_n , premiers à f_n . On peut écrire :

$$x_n = \left(1/f_n^{\varphi(\ell^n)}\right) \left(\sum_a a^{\varphi(\ell^n)} \left(\frac{L_n}{a}\right) - \sum_a a^{\varphi(\ell^n)} b^{\varphi(\ell^n)} \left(\frac{L_n}{b}\right) \left(\frac{L_n}{a}\right)\right).$$

Définissons a' par $\begin{cases} ba' \equiv a \pmod{f_n} \\ 1 \leq a' \leq f_n \end{cases}$

Il est clair que $a \rightarrow a'$ réalise une permutation de l'ensemble des entiers premiers à f_n et compris entre 1 et f_n . Nous aurons donc :

$$x_n = \left(1/f_n^{\varphi(\ell^n)}\right) \left(\sum_a a^{\varphi(\ell^n)} \left(\frac{L_n}{a}\right) - \sum_a a'^{\varphi(\ell^n)} b^{\varphi(\ell^n)} \left(\frac{L_n}{b}\right) \left(\frac{L_n}{a'}\right)\right)$$

$$\text{d'où } x_n = \left(1/f_n \varphi(\ell^n)\right) \sum_a [a^{\varphi(\ell^n)} - a' \varphi(\ell^n) b^{\varphi(\ell^n)}] \left(\frac{L_n}{a}\right).$$

Il apparaît clairement dans cette écriture que x_n appartient à $\mathbb{Z}_\ell[G_n]$. Mais $x^* \left(\frac{L_n}{a}\right)$ est le résidu modulo ℓ^n de a . Donc l'image du résidu modulo ℓ^n de x_n par l'involution du miroir est le résidu modulo ℓ^n de $\bar{x}_n$ défini par :

$$\bar{x}_n = \left(1/f_n \varphi(\ell^n)\right) \sum_a a [a^{\varphi(\ell^n)} - a' \varphi(\ell^n) b^{\varphi(\ell^n)}] \left(\frac{L_n}{a}\right)^{-1}.$$

Calculons maintenant la quantité entre crochets : Nous pouvons écrire :

$$a^{\varphi(\ell^n)} - a' \varphi(\ell^n) b^{\varphi(\ell^n)} = (a - a' b) A \text{ avec}$$

$$A = a^{\varphi(\ell^n)-1} + a' b a^{\varphi(\ell^n)-2} + \dots + (a' b)^{\varphi(\ell^n)-1}.$$

Mais si $a' b = a + \lambda \ell^n$, nous avons alors

$$(a' b)^i = a^i + i a^{i-1} \lambda \ell^n + \dots \equiv a^i + i a^{i-1} \lambda \ell^n \pmod{\ell^{2n}}.$$

Remplaçons dans A : nous obtenons alors

$$A \equiv \varphi(\ell^n) a^{\varphi(\ell^n)-1} + a^{\varphi(\ell^n)-2} (1 + 2 + \dots + (\varphi(\ell^n) - 1)) \lambda \ell^n \pmod{\ell^{2n}}.$$

$$\text{D'où } A \equiv \varphi(\ell^n) a^{\varphi(\ell^n)-1} \pmod{\ell^{2n-1}} \text{ et}$$

$$A/\varphi(\ell^n) \equiv a^{\varphi(\ell^n)-1} \pmod{\ell^n} \text{ et enfin}$$

$$a A/\varphi(\ell^n) \equiv a^{\varphi(\ell^n)} \equiv 1 \pmod{\ell^n}.$$

$$\text{Nous obtenons donc : } \bar{x}_n \equiv (1/f_n) \sum_a (a - a' b) \left(\frac{L_n}{a}\right)^{-1} \pmod{\ell^n}.$$

Il reste à constater que cette dernière quantité n'est autre que y_n .

$$\text{En effet, on a : } y_n = \left(1 - b \left(\frac{L_n}{b}\right)^{-1}\right) (1/f_n) \sum_a a \left(\frac{L_n}{a}\right)^{-1}$$

$$= (1/f_n) \left(\sum_a a \left(\frac{L_n}{a}\right)^{-1} - \sum_a a b \left(\frac{L_n}{a}\right)^{-1} \left(\frac{L_n}{b}\right)^{-1}\right). \text{ Nous raisonnons alors de la}$$

même façon qu'au début de la démonstration : on peut remplacer dans la dernière somme a par a' et on obtiendra :

$$y_n = (1/f_n) \left(\sum_a a \left(\frac{L_n}{a}\right)^{-1} - \sum_a a' b \left(\frac{L_n}{a'}\right)^{-1} \left(\frac{L_n}{b}\right)^{-1}\right) = (1/f_n) \sum_a (a - a' b) \left(\frac{L_n}{a}\right)^{-1}.$$

Proposition 3.6. On suppose toujours que n est ^{un} entier non nul, supé-

rieur à n_1 . Si g est une puissance de ℓ , on suppose de plus que n est supérieur à $n_0 + 1$. Alors le groupe de Galois $\text{Gal}(M_n^n/L_n)$, considéré comme $\mathbb{Z}_\ell[G_n]$ -module, est annulé par x_n^1 .

Démonstration. Les résidus modulo ℓ^n de $\sum_a \left(\frac{L_n}{a}\right)$ et $\sum_a a \left(\frac{L_n}{a}\right)^{-1}$ se correspondent par l'involution du miroir. On déduit donc de la proposition précédente (3.5) que les résidus de x_n^1 et y_n^1 se correspondent par l'involution du miroir. On déduit alors des propositions 3.3 et 3.4 que x_n^1 annule $\text{Gal}(M_n^n/L_n)$.

Remarque. On peut constater que $\sum_a \left(\frac{L_n}{a}\right)^{-1}$ annule $\text{Gal}(M_n^n/L_n)$ et en déduire que x_n annule $\text{Gal}(M_n^n/L_n)$. D'où finalement, on constate que y_n annule $W_n / (L_n^*)^{\ell^n}$. Pourquoi avoir introduit s_n^1 , x_n^1 , y_n^1 ? Uniquement à cause de l'annulation de l'idéal $\mathfrak{b}$ au cours de la démonstration de la proposition 3.3. En effet, nous avons vu à ce niveau que $\mathfrak{b}^{y_n^1} = 1$. Il ne nous a pas semblé très simple de montrer directement que $\mathfrak{b}^{y_n}$ est la puissance $(\ell^n)^{\text{ème}}$ d'un idéal principal.

Introduisons la notation suivante: S_n est l'élément de $\mathbb{Q}_\ell^{(g)}$ défini par $S_n = \left(1/f_n \varphi(\ell^n)\right) \sum_a a^{\varphi(\ell^n)} \chi(a)$. La somme est étendue aux entiers a , compris entre 1 et f_n et premiers à f_n . D'autre part, on considère dans la suite χ comme un caractère de G_n ou de $\text{Gal}(\mathbb{Q}^{(f_n)}_n/\mathbb{Q})$. La valeur $\chi(a)$ est par définition égale à $\chi\left(\frac{L_n}{a}\right)$; cela provient de l'identification de $\text{Gal}(\mathbb{Q}^{(f_n)}_n/\mathbb{Q})$ et de $(\mathbb{Z}/f_n\mathbb{Z})^*$.

Proposition 3.7. Supposons que g n'est pas une puissance de ℓ . Soit n un entier non nul, supérieur à n_1 . Alors S_n appartient à $\mathbb{Z}_\ell^{(g)}$ et annule le

$\mathbb{Z}_\ell^{(g)}$ -module $\mathcal{H}(\chi) / \mathcal{H}(\chi)\ell^n$.

Démonstration. Imposons de plus à l'entier b la condition suivante : $\chi(b)$ est une racine de 1 d'ordre non puissance de ℓ . Nous avons

$\chi_1(x_n) = (1 - b^{\varphi(\ell^n)} \chi(b)) S_n$ et $1 - \chi(b)$ est une unité de $\mathbb{Z}_\ell^{(g)}$. Mais nous avons $1 - b^{\varphi(\ell^n)} \chi(b) \equiv 1 - \chi(b) \pmod{\ell^n}$ et $1 - b^{\varphi(\ell^n)} \chi(b)$ est une unité de $\mathbb{Z}_\ell^{(g)}$. Comme x_n appartient à $\mathbb{Z}_\ell[G_n]$, $\chi_1(x_n)$ appartient à $\mathbb{Z}_\ell^{(g)}$ et S_n également.

D'autre part, on déduit des propositions 3.2 et 3.6 que x'_n annule $\mathcal{H}(\chi) / \mathcal{H}(\chi)\ell^n$. En termes de $\mathbb{Z}_\ell^{(g)}$ -modules, cela veut dire que $\chi_1(x'_n)$ annule $\mathcal{H}(\chi) / \mathcal{H}(\chi)\ell^n$.

Il reste donc à vérifier que $\chi_1(x_n) = \chi_1(x'_n)$. En effet, $\chi_1(x_n - x'_n) = \frac{1}{2}(1 - b) \sum_a a \chi(a)^{-1}$. Comme χ est un caractère réel, on a $\chi(a) = \chi(f_n - a)$ et on en déduit $\chi_1(x'_n - x_n) = 0$. Nous avons démontré la proposition.

Nous pouvons maintenant justifier le théorème A : en effet, le groupe $\mathcal{H}(\chi)$ est fini. Donc si n est assez grand, $\mathcal{H}(\chi)\ell^n$ est égal à 1 et $\mathcal{H}(\chi)$ est annulé par S_n . Il reste alors à utiliser l'approximation ℓ -adique de $L_\ell(1, \chi)$ telle qu'elle est donnée par Fresnel dans [1]. On a $-L_\ell(1, \chi) = \lim_{n \rightarrow \infty} S_n$. Donc $L_\ell(1, \chi)$ annule $\mathcal{H}(\chi)$.

Proposition 3.8. Supposons que g est une puissance de ℓ . Soit n un entier supérieur à n_1 et $n_0 + 1$. Soit ζ_g une racine primitive $g^{\text{ème}}$ de 1. Alors $(1 - \zeta_g) S_n$ appartient à $\mathbb{Z}_\ell^{(g)}$ et annule le $\mathbb{Z}_\ell^{(g)}$ -module $\mathcal{H}(\chi) / \mathcal{H}(\chi)\ell^n$.

Démonstration. Nous imposons maintenant à b de vérifier la condition suivante : $\chi(b)$ est une racine primitive de 1, d'ordre g . Alors, les idéaux de $\mathbb{Z}_\ell^{(g)}$ engendrés par $1 - \chi(b)$ et $1 - \zeta_g$ sont les mêmes : à savoir l'idéal maximal de $\mathbb{Z}_\ell^{(g)}$. On déduit de la congruence $1 - b^{\varphi(\ell^n)} \chi(b) \equiv 1 - \chi(b) \pmod{\ell^n}$, que $(1 - b^{\varphi(\ell^n)} \chi(b)) / (1 - \zeta_g)$ est une unité de $\mathbb{Z}_\ell^{(g)}$. Comme x_n appartient à $\mathbb{Z}_\ell[G_n]$, $\chi_1(x_n)$ appartient à $\mathbb{Z}_\ell^{(g)}$ et $(1 - \zeta_g)S_n$ également. Ces deux éléments engendrent dans $\mathbb{Z}_\ell^{(g)}$ le même idéal. D'autre part, on déduit des propositions 3.2 et 3.6 que $x_n^!$ annule $\mathcal{H}(\chi) / \mathcal{H}(\chi)^{\ell^n}$. Ceci implique que $\chi_1(x_n^!)$ annule $\mathcal{H}(\chi) / \mathcal{H}(\chi)^{\ell^n}$. On a aussi, comme précédemment, $\chi_1(x_n) = \chi_1(x_n^!)$. Ceci démontre la proposition 3.8. Le théorème B s'en déduit de la même façon que le théorème A se déduisait de la proposition 3.7.

Remarque. Nous avons vu au cours de la démonstration de la proposition 3.7, que si g n'est pas une puissance de ℓ , alors S_n appartient à $\mathbb{Z}_\ell^{(g)}$. On peut constater d'autre part, que si f n'est pas une puissance de ℓ , alors S_n appartient à $\mathbb{Z}_\ell^{(g)}$.

Démonstration. Pour tout entier a , premier à f_n , il existe des entiers a' et a'' uniques tels que : $a \equiv a' a'' \pmod{f_n}$; $a' \equiv 1 \pmod{f_0}$; $a'' \equiv 1 \pmod{\ell^n}$; $1 \leq a' < f_n$ et $1 \leq a'' < f_n$. Nous aurons donc $a^{\varphi(\ell^n)} \equiv a'^{\varphi(\ell^n)} a''^{\varphi(\ell^n)} \pmod{\ell^{2n-1}}$ et on en déduit

$$\sum_a a^{\varphi(\ell^n)} \chi(a) \equiv \left(\sum_{a'} a'^{\varphi(\ell^n)} \chi(a') \right) \left(\sum_{a''} a''^{\varphi(\ell^n)} \chi(a'') \right) \pmod{\ell^{2n-1}}.$$

La première somme est étendue aux entiers a , de 1 à f_n , premiers à f_n ; la deuxième aux entiers a' , de 1 à f_n , premiers à f_n , congrus à 1 modulo f_0 et la troisième aux entiers a'' , de 1 à f_n , premiers à f_n , congrus à 1 modulo ℓ^n . Considérons la dernière somme : Nous avons

$$a''^{\varphi(\ell^n)} \equiv 1 \pmod{\ell^{2n-1}}. \text{ Donc } \sum_{a''} a''^{\varphi(\ell^n)} \chi(a'') \equiv \sum_{a''} \chi(a'') \pmod{\ell^{2n-1}}.$$

Mais si f_0 est différent de 1, cette dernière somme est nulle. On a donc

$$\sum_{\mathfrak{a}} \mathfrak{a}^{\varphi(\ell^n)} \chi(\mathfrak{a}) \equiv 0 \pmod{(\ell^{2n-1})} \text{ et ceci montre que } S_n \text{ appartient à } \mathbb{Z}_{\ell}^{(g)}.$$

4. Dernières remarques.

Examinons les approximations de $L_{\ell}(1, \chi)$ fournies par les quantités S_n .

Proposition 4.1. L'entier n est toujours supposé non nul et supérieur à n_1 . Si g n'est pas une puissance de ℓ , alors on a la congruence $S_{n+1} \equiv S_n \pmod{(\ell^n)}$. Si g est une puissance de ℓ et si f n'est pas une puissance de ℓ , alors on a $(1 - \zeta_g) S_{n+1} \equiv (1 - \zeta_g) S_n \pmod{(\ell^n)}$. Si f et g sont des puissances de ℓ , on a seulement $(1 - \zeta_g)^2 S_n \equiv (1 - \zeta_g)^2 S_{n+1} \pmod{(\ell^n)}$.

Démonstration. On choisit l'entier b comme il est indiqué dans les démonstrations des propositions 3.7 et 3.8. Ce choix fait pour n , convient aussi pour $n+1$. Considérons la restriction de $\mathbb{Z}[G_{n+1}]$ à $\mathbb{Z}[G_n]$. Un calcul élémentaire montre que l'image de y'_{n+1} par cette restriction est y'_n ; (Théorème II 3 [2]). D'autre part, si l'on considère la restriction de $A_{n+1}[G_{n+1}]$ à $A_n[G_n]$ et les involutions du miroir relatives à $L_{n+1}/\mathbb{Q}$ et $L_n/\mathbb{Q}$, on constate que ces opérations permutent. Il découle de la proposition 3.5 que le résidu modulo ℓ^n de x'_n coïncide avec le résidu modulo ℓ^n de la restriction de x'_{n+1} à $\mathbb{Z}_{\ell}[G_n]$. Notant de la même façon : χ , le caractère χ de G , son prolongement à G_n et son prolongement à G_{n+1} et notant de la même façon : χ_1 les prolongements $\mathbb{Z}_{\ell}$ -linéaires de χ à $\mathbb{Z}_{\ell}[G_{n+1}]$ et $\mathbb{Z}_{\ell}[G_n]$, nous avons donc $\chi_1(x'_n) \equiv \chi_1(x'_{n+1}) \pmod{(\ell^n)}$. C'est-à-dire : $(1 - b^{\varphi(\ell^n)} \chi(b)) S_n \equiv (1 - b^{\varphi(\ell^{n+1})} \chi(b)) S_{n+1} \pmod{(\ell^n)}$. Mais nous avons $1 - b^{\varphi(\ell^n)} \chi(b) \equiv 1 - \chi(b) \pmod{(\ell^n)}$ et $1 - b^{\varphi(\ell^{n+1})} \chi(b) \equiv 1 - \chi(b) \pmod{(\ell^{n+1})}$.

Lorsque f ou g n'est pas une puissance de ℓ , on en déduit à l'aide de la remarque placée à la fin du paragraphe 3, la congruence

$(1-\chi(b))S_n \equiv (1-\chi(b))S_{n+1} \pmod{\ell^n}$. Si g n'est pas une puissance de ℓ , alors $1-\chi(b)$ est une unité de $\mathbb{Z}_\ell^{(g)}$; d'où $S_n \equiv S_{n+1} \pmod{\ell^n}$. Si g est une puissance de ℓ et si f n'est pas une telle puissance, alors $(1-\chi(b))/(1-\zeta_g)$ est une unité de $\mathbb{Z}_\ell^{(g)}$; d'où $(1-\zeta_g)S_n \equiv (1-\zeta_g)S_{n+1} \pmod{\ell^n}$. Si, enfin, f et g sont des puissances de ℓ , alors $(1-\zeta_g)S_n$ appartient à $\mathbb{Z}_\ell^{(g)}$ et on obtient alors le résultat annoncé en utilisant les mêmes arguments.

Conséquence. On déduit de la proposition 4.1 la convergence de la suite S_n . De plus, le résidu modulo ℓ^n de $L_\ell(1, \chi)$ (ou $(1-\zeta_g)L_\ell(1, \chi)$, ou $(1-\zeta_g)^2 L_\ell(1, \chi)$ suivant les cas) est l'opposé du résidu de S_n (ou $(1-\zeta_g)S_n$ ou $(1-\zeta_g)^2 S_n$). Pour obtenir celui-ci, on peut utiliser le calcul effectué dans la proposition 3.5. En effet, on a, en reprenant les notations adoptées lors de la démonstration de cette proposition :

$$S_n = \left(1/f_n \varphi(\ell^n)\right) \sum_a a^{\varphi(\ell^n)} \chi(a)$$

$$\text{et } (1-b^{\varphi(\ell^n)} \chi(b))S_n = \left(1/f_n \varphi(\ell^n)\right) \sum_a (a^{\varphi(\ell^n)} - a^{\varphi(\ell^n)} b^{\varphi(\ell^n)}) \chi(a).$$

Mais d'après la proposition 3.5, on a aussi :

$(1-b^{\varphi(\ell^n)} \chi(b))S_n \equiv (1/f_n) \sum_a a^{-1} (a - a^{\varphi(\ell^n)} b^{\varphi(\ell^n)}) \chi(a) \pmod{\ell^n}$; en désignant par a^{-1} un entier, inverse de a modulo ℓ^n . Cette formule permet de calculer plus facilement le résidu modulo ℓ^n de $L_\ell(1, \chi)$. (G. Gras a dernièrement généralisé ces considérations et obtenu de façon analogue le résidu modulo ℓ^n de $L_\ell(s, \chi)$: "Sur la construction des fonctions L p -adiques abéliennes" ; à paraître au Séminaire D.P.P.).

Examinons le cas particulier où f et g sont des puissances de ℓ :

Proposition 4.2. Supposons que f et g soient tous deux des puissances de ℓ . On a alors $K = \mathbb{Q}_{n_0} = \mathbb{Q}_{n_1}$. Le corps N est égal à $\mathbb{Q}_{n_0+1}$ et $\mathcal{X}(x)$ est réduit à 1. D'autre part $(1-\zeta_g)L_\ell(1, \chi)$ est une unité de $\mathbb{Z}_\ell^{(g)}$.

Démonstration. La première assertion de cet énoncé est évidente.

Posons pour simplifier $n = n_0 = n_1$. Le degré de χ est donc $g = \ell^{n-1}$ et son conducteur $f = \ell^n$. Nous voulons montrer maintenant que $(1 - \zeta_g) L_\ell(1, \chi)$ est une unité de $\mathbb{Z}_\ell^{(g)}$. Choisissons d'abord un entier b . Pour que $\chi(b)$ soit une racine primitive $g^{\text{ème}}$ de 1, il est suffisant de prendre $b = 1 + \ell$, ou bien tout entier congru à 1 modulo ℓ et non congru à 1 modulo ℓ^2 . Utilisons la suite exacte :

$$0 \rightarrow (1 - \zeta_g) \mathbb{Z}_\ell^{(g)} \rightarrow \mathbb{Z}_\ell^{(g)} \xrightarrow{\alpha} \mathbb{Z}_\ell / \ell \mathbb{Z}_\ell \rightarrow 0,$$

où l'homomorphisme α est défini par $\alpha\left(\sum_i c_i \zeta_g^i\right) = \sum_i c_i + \ell \mathbb{Z}_\ell$ (les c_i sont

dans $\mathbb{Z}_\ell$). Considérons l'élément de $\mathbb{Z}_\ell^{(g)}$: $(1 - b^{\varphi(\ell^n)} \chi(b)) S_n$ et calculons

son image par α . Pour cela il est nécessaire d'écrire cet élément comme combinaison linéaire à coefficients dans $\mathbb{Z}_\ell$ de 1, ζ_g , ζ_g^2 , ... etc. Comme

au début de la démonstration de la proposition 3.5, nous écrivons ($\sum_a$ a le

même sens) $(1 - b^{\varphi(\ell^n)} \chi(b)) \sum_a a^{\varphi(\ell^n)} \chi(a) = \sum_a (a^{\varphi(\ell^n)} - a^{\varphi(\ell^n)} b^{\varphi(\ell^n)}) \chi(a)$ et

$a^{\varphi(\ell^n)} - a^{\varphi(\ell^n)} b^{\varphi(\ell^n)} \equiv 0 \pmod{\ell^{2n-1}}$. L'image par α cherchée est donc la

classe modulo ℓ de $(\sum_a a^{\varphi(\ell^n)} - a^{\varphi(\ell^n)} b^{\varphi(\ell^n)}) / f_n \varphi(\ell^n)$. Le même calcul

montre que cette expression est la classe modulo ℓ de

$(1 - b^{\varphi(\ell^n)}) (1 / f_n \varphi(\ell^n)) \sum_a a^{\varphi(\ell^n)}$. Or il est facile de vérifier que cet élé-

ment de $\mathbb{Z}_\ell$ est premier à ℓ : en effet, puisque $b \not\equiv 1 \pmod{\ell^2}$, on a

$b^{\varphi(\ell^n)} \not\equiv 1 \pmod{\ell^{n+1}}$ et $(1 - b^{\varphi(\ell^n)}) / f_n$ est une unité de $\mathbb{Z}_\ell$. De même,

$a^{\varphi(\ell^n)} \equiv 1 \pmod{\ell^n}$ et $\sum_a a^{\varphi(\ell^n)} \equiv \varphi(\ell^n) \pmod{\ell^n}$, montre que $(\sum_a a^{\varphi(\ell^n)}) / \varphi(\ell^n)$

est aussi une unité de $\mathbb{Z}_\ell$. On déduit donc de la suite exacte écrite plus haut que

$(1 - b^{\varphi(\ell^n)} \chi(b)) S_n$ est une unité de $\mathbb{Z}_\ell^{(g)}$. Il en sera de même de $(1 - \zeta_g) S_n$.

D'après la proposition 4.1, $(1 - \zeta_g) L_\ell(1, \chi)$ est aussi une unité de $\mathbb{Z}_\ell^{(g)}$.

Il découle alors du théorème B que le groupe $\mathcal{H}(\chi)$ est réduit à 1 et que le corps N est égal à $\mathbb{Q}_{n+1}$.

Bibliographie.

- [1] Fresnel J. Nombres de Bernoulli et fonctions L p-adiques, Ann. Inst. Fourier, 17, 2 (1967), 281-333.
- [2] Gras G. Application de la notion de φ -objet à l'étude du groupe des classes d'idéaux des extensions abéliennes, Publications mathématiques de la Faculté des Sciences de Besançon 1975-1976.
- [3] Gras G. Annulation du groupe des ℓ -classes généralisées d'une extension abélienne réelle de degré premier à ℓ , Ann. Inst. Fourier, 29, 1, (1979).
- [4] Leopoldt H. W. Zur Struktur der ℓ -Klassengruppe galoischer Zahlkörper, Journ. für die reine und ang. Math. 199 (1958).
- [5] Oriat B. et Satgé P. Un essai de généralisation du "Spiegelungssatz", Journ. für die reine und ang. Math. 307 (1979).

Bernard Oriat

Mathématiques E. R. A. n°070654

Faculté des Sciences

25030 BESANCON Cedex

